CYBERATTACKS AND PUBLIC OPINION: THE EFFECT OF UNCERTAINTY IN GUIDING PREFERENCES

Eric Jardine[a], Nathaniel Porter[b] & Ryan Shandler[c]

Accepted Manuscript:

Journal of Peace Research

This article is the introduction to a dedicated special issue on the topic of:
Cyber-Conflict - Moving from Speculation to Investigation

The full article can be found at:
https://doi.org/10.1177/00223433231218178

[a] Chainanalysis

[b] Virginia Tech, University Libraries & Department of Sociology

[c] Georgia Institute of Technology, School of Cybersecurity & Privacy

Corresponding Author: rshandler@gatech.edu
The dataset and statistical replication files for the empirical analysis in this article are available at https://www.prio.org/jpr/datasets/
This publication is not affiliated with Chainalysis and the views represented herein are those of respective authors.

Abstract

When it comes to cybersecurity incidents - public opinion matters. But how do voters form opinions in the aftermath of cyberattacks that are shrouded in ambiguity? How do people account for uncertainty inherent in cyberspace to forge preferences following attacks? This paper seeks to answer these questions by introducing an *uncertainty threshold mechanism* predicting the level of attributional certainty required for the public to support economic, diplomatic or military responses following cyberattacks. Using a discrete-choice experimental design with 2,025 U.S. respondents, we find lower attributional certainty is associated with less support for retaliation, yet this mechanism is contingent on the suspected identity of the attacker and partisan identity. Diplomatic allies possess a reservoir of good-will that amplifies the effect of uncertainty, while rivals are less often given the benefit of the doubt. We demonstrate that uncertainty encourages the use of cognitive schemas to overcome ambiguity, and that people fall back upon pre-existing and politically guided views about the suspected country behind an attack. If the ambiguity surrounding cyberattacks has typically been discussed as an operational and strategic concern, this paper shifts the focus of attention to the human level and positions the mass public as a forgotten yet important party during cyber conflict.

Keywords: cyber conflict, public opinion, uncertainty, retaliation, attribution

Introduction

When it comes to cybersecurity incidents - *public opinion matters* (Shandler & Canetti, 2023). You mightn't know this from a review of the cyber conflict literature, where prominent debates often ignore the public. One flashpoint regards the decision whether cyberspace is a new strategic domain or in fact a continuation of intelligence contests (Gartzke & Lindsay, 2015, Brantly, 2016, Rovner, 2019, Maschmeyer, 2021). Another prominent debate questions whether cyber operations complement or substitute for military operations (Kostyuk & Gartzke, 2022; Schneider, Schechter & Shaffer, 2022; Egloff & Shires, 2021). Still another conceptual dispute focuses on the (de)escalatory properties of cyber conflict (Healey & Jervis, 2020; Libicki & Tkacheva, 2020; Maschmeyer, 2023b; Valeriano & Jensen, 2022). While these crucial debates play out at strategic, operational and international levels, a forgotten actor has fallen by the wayside --- the general public.

It is easy to dismiss the relevance of public opinion when it comes to cybersecurity. Intricate dynamics of international relations take place above the heads of regular voters, who have historically deferred to co-partisan elites in matters of international relations (Berinsky, 2009). Moreover, the sheer complexity of cyberspace can leave the public at a loss. Yet for all their credulity, the public maintains a crucial role surrounding cybersecurity (Shandler, Kostyuk & Oppenheimer, 2023). Widespread exposure to cyberattacks has been shown to undermine trust in government (Gross, Canetti, and Vashdi 2016; Shandler & Gomez, 2023), generate support for intrusive surveillance policies at the expense of civil liberties (Snider et al., 2021; Arsenault et al., 2023), and provoke public demands for retaliatory action that can place pressure on elected officials to escalate tensions (Leal and Musgrave 2023; Shandler et al., 2022). On top of this, mounting evidence has demonstrated decision makers are

at least somewhat responsive to public attitudes toward conflict (Sevenans, 2021; Lin-Greenberg, 2021; Tomz & Weeks, 2020). Put simply, the general public's reactions to cyberattacks can be politically consequential.

These outcomes are not mere scholarly conjecture. In a vivid case study, Baram (2023) described how an Iranian cyberattack against Israeli water infrastructure was publicly revealed by Israeli authorities in part "*to offset the humiliation caused by the public exposure and to control the narrative surrounding the incident" (p. 13).* Authorities exhibited acute sensitivity to public reactions to cyberattacks, and indeed, intense public demands for retaliatory strikes weighed upon decision makers.

But how do voters form opinions in the aftermath of cyberattacks that are shrouded in ambiguity? How do people account for the extensive uncertainty inherent in cyberspace to forge political attitudes following attacks? Common sense dictates voters should exhibit restraint in forming policy positions when the facts of an attack remain unclear. If authorities are not fully certain who is behind an attack, or whether the disruption was an attack at all, voters should logically delay adopting extreme policy positions or demanding retaliation until the full picture emerges. However, the general public is not renowned for calmly and patiently collecting full information before forming positions. Voters react to security incidents in the heat of the moment, when uncertainty is rife, and in the context of typically hyperbolic media reporting (Loewenstein & O'Donoghue, 2007).

This study therefore examines how the public grapples with uncertainty surrounding cybersecurity incidents, focusing on attributional uncertainty --- a facet of uncertainty characteristic of cyberspace. We theorize that greater uncertainty about a cyber attacker's identity will reduce the extremity of public calls for revenge --- and that in the context of incomplete information, people will employ information shortcuts to form political judgements. Specifically, we assert that the effect of uncertainty depends on the suspected identity of the country in question, and the forms of available responses. With this in mind, we introduce and empirically test an uncertainty threshold mechanism that predicts and explains at what level of certainty, and under what conditions, the attributional uncertainty dilemma will restrain public demands for economic, diplomatic or military responses.

We examine this mechanism by conducting a survey experiment that exposes voters to cyberattack scenarios under various thresholds of uncertainty, before gauging the extent of demands for economic, diplomatic, or military responses. Reflecting the exaggerated language employed by media outlets, our experimental scenarios depict a rich variety of cyberattacks, ranging from minor attacks that cause no physical consequences or economic damage, to major attacks against critical infrastructure. Our primary predictor variable is the authorities' level of certainty as to the identity of the cyber attacker. For example, once it is concluded that there is a 60% likelihood that Russia is behind an attack, what does one do with that information? What would happen if it were 70% instead? What threshold of certainty is required for people to support some retaliatory response, and what psychological and situational factors guide this decision pathway?

To probe uncertainty's influence on a broad spectrum, we employ a ratings-based conjoint experimental design on a nationally representative sample of United States respondents (N = 2,025). The data reveal that medium to low levels of certainty about who launched a malicious cyber operation dramatically reduces the likelihood the public will support even minor retaliatory options. However, the exact threshold of this uncertainty mechanism is contingent on the suspected identity of the attacker and partisan identification. We demonstrate that diplomatic allies of the United States enjoy a reservoir of goodwill that that inhibits support for retaliation provided there is any uncertainty about the identity of the attacker in the public's mind. By contrast, retaliation against rivals is accepted in the face of far lower certainty.

Our findings emphasize the need to pay attention to a frequently overlooked stakeholder in the cyber conflict literature – the general public. The public experience cyberattacks as enormously threatening and anxiety-provoking (Shandler, Snider & Canetti, 2022). When cyberattacks spill over to critical infrastructure, the public is unlikely to simply ignore the attack as acceptable sub-crisis manoeuvring. To the extent the public wields at least some influence on foreign policy decisions in the aftermath of attacks, their responses cannot be disregarded. In this light, our findings reinforce the public's role during conflict and suggests that the exaggerated public experience of cyber conflict may pressure political elites, who would otherwise be willing to dismiss many cyberattacks, toward retaliation.

A Spectrum of Attributional Uncertainty in Cyberspace

The attribution dilemma in cyberspace refers to the common assumption that cyber attackers can obscure their identity due to the underlying architecture of the Internet (Boebert, 2010; Rid & Buchanan, 2015). Several factors can impede effective attribution. Technical design features of the Internet itself make tracing the source of an attack challenging, particularly if adversaries employ basic obfuscation (Clark & Landau, 2011). Malicious actors might also work via arm's length cyber mercenaries to ensure plausible deniability (Maurer, 2018). Moreover, the sheer complexity of modern cyberattacks means gleaning clues to an attacker's identity requires extensive expertise, and the prodigious data often available can give rise to contradictory results.

Although attribution questions pervade all security crises, the dilemma is particular idiosyncratic of cyberspace. Physical or sovereign borders cannot effectively impede cybernetic attacks, and transnational reliance on common systems underpinning digital systems allows actors to easily project force (Fischerkeller & Harknett, 2017). This issue is compounded by the proliferation of state and non-state entities capable of conducting attacks. While only a few actors have access to intercontinental missiles, for example, the same cannot be said for computer code.

However, the perceived complexity of attributing cyberattacks has steadily eroded during the last decade. Rid & Buchanan (2015) argued that even without irrefutable technical evidence, states can match a cyber offender to an offence by combining tactical, operational and strategic analyses. Even if the pool of potential attackers is vast, cross-referencing those with capability and geo-political interest in waging an attack can assist attribution (Blagden, 2020; Rid & Buchanan, 2015). In fact, successfully identifying the parties responsible for cyberattacks is more common than people think (Boebert, 2010; Lupovici, 2016) – especially for the highest-profile attacks, where private cybersecurity companies supplement state analyses (Egloff, 2020b). While identifying the group or authority ultimately responsible for an attack remains a challenge, it is often solvable with enough time, expertise and will (Lin, 2016).

As sensationalist proclamations of inscrutable hackers have given way to more nuanced understandings of attributional processes, we have learned to avoid simplistic conceptualizations on an artificially binary scale. The "process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades" (Rid & Buchanan, 2015). This difficulty associated with attribution is not unique to cyberspace. Technical evidence is usually not sufficient to assign responsibility in other domains of international conflict, which are similarly fraught with an interplay of material evidence and inferential processes. Even with bullets, missiles and biological attacks, analysts can rarely provide 100% certainty about who is ultimately responsible for giving an order to attack. For example, a bio-terror attack in 2001 took place when numerous letters containing anthrax spores were mailed to media outlets in Florida and New York. Five people were killed. Yet despite concrete evidence and extensive chemical and biological analyses, analysts could not

immediately and definitively identify the attacker (Koblentz & Tucker, 2010). Attribution is a complex art in all domains. However, the absence of definitive assurance does not prevent political leaders and military officials from responding to attacks. They and we have learned to incorporate some uncertainty into decision making processes. In this light, it is incumbent upon us to incorporate a spectrum of uncertainty into our cyber-attribution dilemmas, and avoid oversimplifying attribution as a binary construct.

How Uncertainty Alters Support for Retaliation – A Situational and Psychological Account

To this point in the paper, our analysis has focused on *sense-making* - the manner by which complex data is converted into attribution judgements (Egloff & Dunn Cavelty, 2021). However, attribution is not the end-point of the process. Attribution is central to cybersecurity politics precisely because it imbues technical phenomena with political consequences, creating truths that guide decision making. Therefore, to understand how attributional uncertainty influences political outcomes, we need to progress to a second and often forgotten step of *meaning-making*. This step explores how attribution judgements exert concrete political effects (Egloff, 2020a). Once an attributional judgement has been made, at a given level of certainty, we can then test how people interpret and act upon these judgements. If the first step is deliberate investigation of the empirical circumstances of an act, the second phase is entirely subjective, making it prone to psychological biases, political pressures, and competing narratives acting upon human decision making (Lindsay, 2015; Egloff & Dunn Cavelty, 2021).

The mass public must frequently grapple with government assessments made with varying degrees of certainty. A model scenario emerged in 2023, where, amid acrimonious discussions on the origins of COVID, the U.S. Energy Department and the FBI published reports concluding that COVID may have leaked from a laboratory, yet noted that the assessment was made with *low or moderate confidence*. Four other agencies declared that the virus arose naturally from an animal, with *low confidence*. The question for us is how people react to the proviso of confidence assessments – whether it exerts any effect, and if so, how strong.

In the context of cyberattacks, it is widely assumed heightened uncertainty will diminish support for retaliation. On the most basic level, retaliating against an innocent actor, whether militarily or by imposing trade sanctions, could have severe consequences, and risk-aversion in foreign policy matters is likely to diminish support for aggressive steps under unclear circumstances (Hansel, 2018). To the extent the public acts rationally, lower attributional certainty should therefore decrease support for retaliation.

However, people don't always act rationally, and emotions exert a strong influence on decision-making - especially in cyberspace (McDermott, 2019). Recent studies have demonstrated that exposure to cyberattacks elicits strong emotional responses that can sway subsequent decision-making (Shandler, Gross & Canetti, 2023; Backhaus et al., 2020; Canetti et al., 2017). Specifically, to the extent that people experience anger following cyberattacks, they tend to lash out against perceived injustice and demand retaliation against responsible parties (Shandler et al., 2022). Despite the centrality of emotional dynamics surrounding cyber threats, the process of converting uncertainty into policy judgement demands cognitive / evaluative processes, and we therefore suggest that uncertainty considerations will be more rational than emotional.

Weighing the above factors, we formulate a pre-registered hypothesis that (H1) *lower attributional certainty will reduce public support for retaliation.* In addition to this primary theoretical expectation, we offer several additional hypotheses to tease out some nuances of when and why uncertainty can exert an

effect on retaliatory preferences. Though these subsequent hypotheses were not pre-registered in advance of the data collection, we find the results persuasive, and offer a theoretical basis for the expectations to allow readers to reach an informed decision as to their validity.

A key factor guiding decision-making surrounding certainty assessments is people's discomfort with complex numerical variables. It is easy to absorb the implications of uncertainty on a binary scale. Either we know who is behind the attack, or we don't. But what does it mean that officials are 70% certain a particular country is responsible for a military strike? If the level of certainty rises to 75% - what weight should we give to that incremental change? Extensive research has demonstrated people struggle to effectively draw meaning from numbers (Peters et al., 2006). Due to people's difficulty with numerical assessments, we further hypothesize that (H2) *respondents will internalize the uncertainty spectrum by treating any attribution above a threshold level as certain, while viewing any attribution below that threshold as uncertain*. For this expectation to be corroborated in our findings, we should see a steep drop off in support for retaliation at one particular level of certainty.

Beyond a general discomfort with complex analyses, there are cognitive schemas specific to cyberspace that guide decision making in the aftermath of cyberattacks (Gomez, 2021; Hansel, 2018). These schemas form fallback tools that facilitate the processing of ambiguous information. For example, Gomez (2019) introduced the concept of 'seizing' in cyberspace – "a pre-disposition to gravitate towards cues that appear to confirm pre-existing belief(s)" (p. 1). This inclination, conceptually similar to more well-known confirmation biases, is associated with the need to maintain cognitive consistency despite uncertainties. As such, we can expect that faced with attributional uncertainty, people will search for cues confirming their existing beliefs. A significant cue in this regard would be their view of the country that is under suspicion. As a general rule, the public copes with a confusing world by adopting images about countries (friend or foe) that help guide their reasoning about world affairs (Brewer et al., 2004; Castano, Bonacossa & Gries, 2016). People use these images as informational shortcuts to form political judgments and interpret confusing or contradictory data.

We therefore hypothesize that (H3) *country images will moderate the effect of attributional uncertainty*. In other words, to contend with attributional uncertainty, people will partly interpret events through the lens of foreign political alliances. For example, if the United Kingdom was suspected with 50% certainty of conducting an attack on the United States, we suggest the American public would grapple with the uncertainty of this claim by falling back upon their pre-existing view of the U.K. as a longstanding US ally. But if China, a rival, were suspected at the same level of certainty, the public would interpret the analysis through the lens of their pre-existing adversarial image of China to reduce cognitive dissonance. As partisanship is highly correlated with people's trust in and view of foreign countries (Brewer, 2004), we further hypothesize that (H4) *the friend or foe heuristic will be contingent upon partisan identity*. Republican foreign policy rhetoric is harsher towards rivals and warmer toward allies than Democratic rhetoric (Ivie & Giner, 2009), meaning any moderating effect of country image should be steeper among Republicans.

A second schema that influences decision making in an environment of uncertainty is people's perception of the mode of military / diplomatic / economic retaliation. While the public is generally willing to support military escalation if the stakes are important and the prospects of victory are favorable, they are less likely to support forceful military retaliation for attacks experienced in the cyber domain (Kreps & Schneider, 2019; cf. Gross et al. 2016; 2017). This may result from increased attributional uncertainty in cyberspace dampening enthusiasm for aggressive retaliatory options (Hedgecock & Sukin, 2023). If the identities of cyber attackers are inherently uncertain, people may prefer retaliatory cyberattacks to cross-domain retaliation. We therefore hypothesize that (H5) *method of retaliation will moderate the effect of attributional uncertainty*. When uncertainty is greater, we expect that

respondents will exhibit higher support for cyber retaliation, and that this relative preference for cyber retaliation will diminish in when the identity of the attack is more certain.

Experimental Design

Traditional experimental techniques would find it difficult to effectively test the effects of a continuum of attributional uncertainty due to statistical power constraints. Since viewing attributional uncertainty on a spectrum is a key theoretical development of this paper, we employ a discrete choice conjoint technique to study how different levels of certainty drive public support for retaliation.[1] A conjoint design allows us to hold fixed a range of additional relevant attributes of incidents that would otherwise confound observational studies. This experimental technique works by constructing randomly generated scenarios with interchangeable values drawn from a prepopulated list of attributes. Each attribute, outlined in figure 1, has between four and nine values that are randomly selected to populate the scenario. For example, the attribute of 'attributional certainty' could be any of nine values on a spectrum from 10% to 90%, while the 'suspected attacker' attribute could be either Russia, China, Israel, India or the United Kingdom. In our conjoint structure, there are 32,400 unique permutations of the scenario that can be assembled by drawing a single value from each attribute.[2]

The survey was distributed to a nationally representative sample of 2,025 respondents in the United States via the Qualtrics survey company.[3] After viewing a scenario describing a cyberattack against the United States – respondents were presented with information about two possible perpetrators. For each suspected country, the randomly allocated information dealt with the certainty of the attribution, the proposed means of retaliating, the costs (economic and human) of retaliating, the chances of conflict escalation, and the identity of the attacker. Each respondent was asked to indicate which course of action they prefer in a head-to-head style matchup: retaliate again possible perpetrator A, retaliate against B, or avoid retaliation at this time. Each respondent evaluated a total of five scenarios, with two suspected attackers and proposed responses in each scenario, amounting to 20,050 retaliatory action decisions. Detailed balance checks and further information on sample demographics appear in Online Appendix A. The experimental design and pre-registered hypotheses were submitted prior to data collection, and the pre-analysis plan appears in the Online Appendix.

Survey Instrument

In the experiment, we manipulate six attributes of a cybersecurity incident involving US critical infrastructure. In addition to level of attributional uncertainty, which forms the center of our investigation, we include six other attributes commonly understood to influence public support for retaliation. Each attribute is listed in Figure 1 and discussed in the text below. An example of the choice options viewed by respondents appears in Online Appendix B.

[1] For an in-depth analysis of the effectiveness of conjoint structures in general, and discrete-choice conjoint designs in particular, see Sniderman (2018).

[2] We add two constraints within the randomization protocols to avoid the possibility of implausible scenarios. Accordingly, scenarios depicting a 'naming and shaming' response did not allow for fatalities as a response outcome. This constraint reduced the pool of possible scenarios from 32,400 unique permutations to 25,920 unique permutations.

[3] The representative sample was constructed using a quota system that matched self-reported sample demographics to the national population according to age, gender, income, region and race. Respondents who failed embedded attention checks or did not complete the survey were removed from the sample.

First, we manipulate the *level of attributional certainty*. We refrain from a pre-emptive binary categorization of certain versus uncertain, preferring to include nine possible values of attributional certainty ranging from 10% to 90% - increasing in 10% increments. We do not include a 0% certainty option, since there is no genuine prospect of retaliation against a country that is not at all suspected as a perpetrator. Likewise, we do not include a 100% certainty option, since this level of certitude is exceedingly rare for cyberattacks where adversaries employ even basic obfuscation steps. The highest level of certainty (90%) was selected as the baseline value against which progressively deteriorating confidence in the identity of the attack can be compared.

Second, we manipulate the identity of the *suspected attacker*. Possible attackers included China, Russia,[4] India, Israel and the United Kingdom. These countries reflect a mix of prominent allies (UK, Israel), rivals (Russia, China), and non-aligned countries (India). The US public holds remarkably consistent attitudes towards foreign countries (Castano, Bonacossa & Gries, 2016), and these countries were included as a result of their ability to evoke instinctively positive or negative views. Right or wrong, Americans have coherent views of friends and foes, and these perceptions shape attitudes towards foreign affairs.

Third, we manipulate the economic *cost of retaliation*. Research has repeatedly shown the public contemplates expected costs of military action in deciding whether to support military strikes (Tomz & Weeks, 2013). This logic extends to other retaliatory action, with higher economic costs leading to lower public support. Our conjoint structure includes four possible predictions of the potential economic cost of retaliation: $100 Million, $500 Million, $1 Billion, and $10 Billion. The lowest figure of up to $100 million serves as the baseline value.

Fourth, we manipulate the *number of potential deaths* expected to arise from any subsequent military escalation of the conflict. Public attitudes towards retaliation are directly associated with expected casualties (Fazal, 2021). Values for this attribute were set to randomly vary from either no US deaths, up to 100, up to 1,000, up to 10,000 or up to 50,000 US deaths. These are not expectations of casualties stemming from a single strike, but rather the cumulative consequence of an escalating incident. Zero deaths serves as the baseline value.

Fifth, we manipulate the *estimated probability of the conflict escalating into a broader conflagration* following the proposed response to the current incident. Similar to financial costs and expected casualties, the public typically evaluates the likelihood of the mission being successful (Gelpi, Feaver & Reifler, 2009). We therefore offer a range of likelihoods that action will lead to further escalation, with values ranging from 10% to 90% by increments of 10%.

Sixth, we manipulate the *proposed method of retaliation*. The public possess keen views about appropriate modes of retaliation, a factor heightened in cyberspace due to people's innate caution about escalating cyberattacks into the physical domain (Kreps & Schneider, 2019; Shandler, Gross & Canetti, 2021). We include four options for retaliation: economic sanctions, naming and shaming the suspected attacker, in-kind cyber response, and military force. As naming and shaming a potential aggressor is the least destructive potential option, this value is the baseline against which the more serious retaliatory choices are compared. To ensure plausibility, when the proposed method was naming and shaming, only the zero-casualty condition was used.

[4] We note that this survey was conducted before the onset of hostilities between the Ukraine and Russia, which considerably harshened American attitudes toward Russia.

Figure 1: Attributes and values in conjoint treatment

Attributes	Values
(A) Certainty they were behind the attack	90% **(*)**
	80%
	70%
	60%
	50%
	40%
	30%
	20%
	10%
(B) Suspected Attacker	China **(*)**
	Russia
	India
	Israel
	United Kingdom
(C) Potential US economic damage of conflict escalation	Up to $100 Million **(*)**
	Up to $500 Million
	Up to $1 Billion
	Up to $10 Billion
(D) Potential US human costs of conflict escalation	No US deaths **(*)**
	Up to 100 US deaths
	Up to 1,000 US deaths
	Up to 10,000 US deaths
	Up to 50,000 US deaths
(E) Chance response will escalate conflict	90% **(*)**
	80%
	70%
	60%
	50%
	40%
	30%
	20%
	10%
(F) Proposed Means of Retaliation	Economic sanctions **(*)**
	Name and shame attacker
	In-kind cyber response
	Military force

Note: This table shows the attributes and values that are used to generate scenarios in the conjoint treatment. Asterisked values in each attribute category designates the 'baseline item' against which all of the other items are measured.

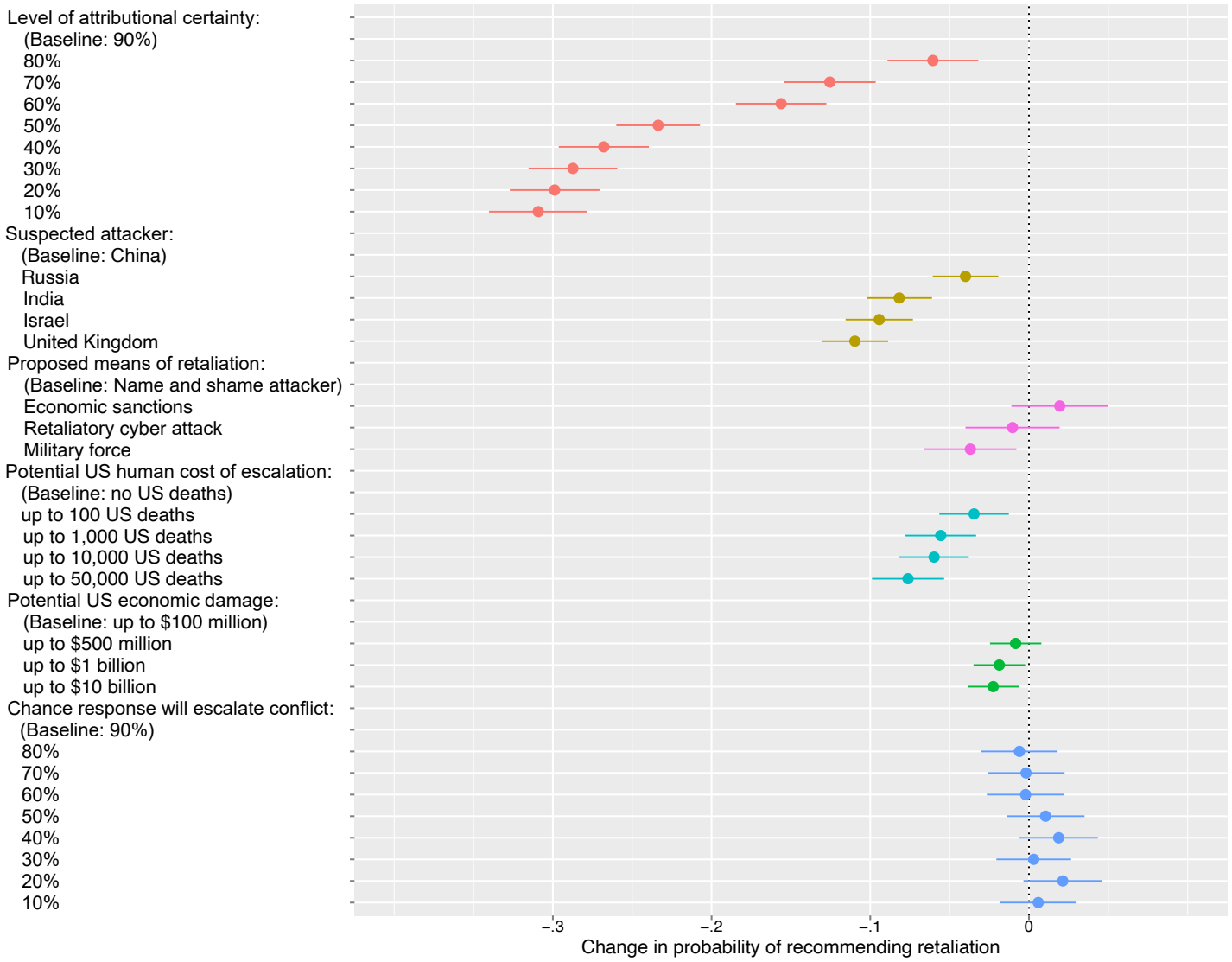
The possible range of scenarios respondents may encounter via our conjoint technique is extremely broad. At one end of the spectrum, a randomly generated scenario might depict a physically destructive attack against critical infrastructure initiated by a state rival that paves the way toward a costly war. At the other end of the spectrum, a scenario might depict a minor cyberattack that causes no major consequences, little economic damage, and provokes a meek response involving the naming and shaming of the attacker. We emphasize that not all of these scenarios are equally likely to occur in reality. The inclusion of unlikely state-on-state attacks is not an endorsement of the discredited 'cyber pearl-harbor' perspective of cyber threats. Rather, we broadly operationalize cyberattacks as having minimalist and maximalist effects in order to test how different scenarios elicit public responses at different levels of severity, and with different levels of attributional certainty.

Results

Figure 2 displays the full conjoint plot showing the relative effect of each attribute. To analyze the respective influence of each value, we look to the average marginal component effects (AMCE). The AMCE statistic calculates the marginal likelihood that the inclusion of a particular value in our scenarios elicits support for retaliation relative to the baseline value in that attribute (Hainmueller and Hopkins, 2015). All standard errors are clustered by respondent in recognition of the fact that rating outcomes are not fully independent when respondents evaluate multiple scenarios. Lines indicate 95% confidence intervals for the AMCE associated with each value.

A number of trends immediately emerge from Figure 2. Taking note of the effect of **attributional certainty**, we can see a clear progression whereby less certainty equates with lower support for retaliation. This corroborates our first hypothesis (H1). On one hand, it is interesting to note that even at the lowest level of certainty – a mere 10%, support for retaliation does not reach zero. Support for reprisal is reduced by 30.9 percentage points (SE = 0.02), from 44.9% support at 90 percent certainty to 14.0% at 10 percent certainty. When retaliation is deemed necessary, the absence of certainty about the identity of the attacker reduces but does not preclude support for an attack. In other words, there is no minimum threshold of attributional certainty that must be met to secure at least some level of public approval for retaliatory action. Yet even while recognizing the limited constraining effect at work, uncertainty nevertheless exerts the largest causal effect on the choice of respondents to support retaliation. For example, raising the spectre that continued escalation may lead to up to 50,000 U.S. deaths only reduces support for retaliation by 7.6 percentage points, barely more than the smallest measured reduction in attribution certainty from 90% to 80%.

Figure 2: Effects of incident attributes on the probability of supporting retaliation



Note: This plot depicts estimates of the effect of the inclusion of each value on the probability of support for retaliation. Estimates are based on the benchmark OLS model with clustered standard errors. Bars represent 95% confidence intervals.

Looking closer at the trendline for uncertainty, we observe two statistically significant discontinuities. For incidents where the attacker's identity is known with a 10% to 50% level of confidence – people exhibit a similar contraction of support for retaliation ranging from 23.4 to 30.9 percentage points. It is not that each consecutive reduction in certainty wipes away an equivalent level of support for retaliation in a linear additive manner. Rather, the public views all assessments at 50%

certainty or less almost interchangeably, under the artificial category of low certainty. By contrast, attributional assessments ranging from 60% to 70% form a middle range and are, in effect, undifferentiable from each other. Eighty percent certainty again qualitatively jumps from the 60% to 70% range, with the reduction of a willingness to retaliate dropping by just over 5 percentage points from the maximal certainty score in our data (90%).

The emergence of two empirical discontinuities in a numerically continuous uncertainty scale accords with our second hypothesis. We expected people's tendency to simplify continuous spectra into discrete categories would lead to the adoption of guiding schema, and we find that the 50% or less, 60-70% and 80% or greater are the crucial levels at which the public ascribed different levels of attributional confidence from the numerical data. While we anticipated a single cut point, the occurrence of two distinct cuts fits with expectations.

Turning to the identity of the **suspected attacker**, we observe a small but significant effect in the influence of country origin. Positing China as the supposed actor responsible for the initial strike leads to the highest level of support for retaliation, with other countries eliciting relatively less support. The effect sizes in Figure 2 suggest respondents have coherent visions of friends and foes on the international stage. Relative to China, accusing Russia as the responsible party reduces support for retaliation by 4.0 percentage points (SE = 0.01), while envisioning the United Kingdom as the attacker sees support fall by a far greater margin (11.0 percentage points, SE = 0.01).

The following three attributes investigate how potential future consequences of retaliation influence support for retaliatory action. Looking at the economic **cost of retaliation** attribute, we see minimal effects. Increasing the projected cost of retaliation to $10 billion only reduces support for retaliatory measures by 2.3 percentage points (SE = 0.01). This finding disputes previous research that positioned economic costs as a variable that strongly influences public support for conflict. While it may be significant in isolation, we demonstrate in the next section that its effects are subsumed by other variables in more complex scenarios.

The **likelihood of further escalation** attribute has no measurable effect. Among the gamut of variables that the public weighs up, they do not place an emphasis on whether retaliation may lead to future escalation. There are several reasons there might be no observable effect here. First, there is potentially only so much uncertainty that people can internalize, and the muted effect for future uncertainty could suggests a bias toward resolving present-setting uncertainty first before speculating about the likelihood of future prospective events. A second interpretation is that responding to an unwarranted attack is a moral imperative in the eyes of the public. Where justice need be served and honor regained, punitive action could be deemed necessary, even if the consequences may propel escalatory pathways.

Looking at another future-oriented attribute, we find evidence that **projected U.S. casualties** that would occur as a result of any military escalation does weight on people's thinking. Forecasting up to 100 U.S. deaths reduces support for retaliation by 3.5 percentage points (SE = 0.01), while increasing the calculation to 50,000 deaths reduces support for retaliation by 7.6 percentage points (SE = 0.01). While this exerts a stronger effect than future economic costs and the risk of escalation, it is notable that the prospect of tens of thousands of U.S. deaths exerts only a minor deterrent effect on public attitudes.

Finally, the **retaliation type** attribute reveals two categories of effects. One category is the non-violent response options, where surprisingly, cyber retaliation is lumped together with naming and shaming the attacker and imposing economic sanctions. A second category is conventional military responses, where the suggestion to launch kinetic strikes reduces support for retaliation by 3.7 percentage points (SE = 0.01). This offers partial support for past findings indicating a heightened

public willingness to back cyber retaliation over conventional military retaliation due to a litany of perceived benefits, including less collateral damage, and greater access to sensitive targets (Shandler, Gross & Canetti, 2021).

Interaction Effects

Recognizing that attributional uncertainty does not operate in a vacuum, we consider several interaction effects. We hypothesized that the uncertainty in cyberspace would arouse a tendency to adopt cues confirming pre-existing beliefs (H3). In international relations, the most relevant guiding schemas are views of countries as either friends or foes. As such, we expect to see the uncertainty effect tempered for allies and inflated for rivals. In Figure 3 we present this interaction effect. We find that certainty's effects are indeed sensitive to pre-existing diplomatic ties – though this interaction primarily occurs where attributional certainty rises into the 'high confidence' territory.

Figure 3: Certainty and country interactions

Attributional Certainty ↓	China	Russia	India	Israel	United Kingdom	Difference in Support for Retaliation: China vs. UK
90	51%	47%	44%	42%	39%	12%
80	46%	43%	36%	37%	32%	14%
70	42%	38%	30%	28%	24%	18%
60	36%	30%	29%	25%	26%	10%
50	30%	26%	19%	16%	16%	14%
40	24%	20%	16%	18%	14%	10%
30	22%	18%	12%	16%	12%	10%
20	20%	17%	16%	9%	12%	8%
10	16%	14%	12%	14%	14%	2%
Mean: 60 - 90	44%	39%	35%	33%	31%	14%
Mean: 10 - 50	22%	19%	15%	15%	14%	9%

Note: Cells indicate the observed rate of support for retaliation at every level of uncertainty for each suspected attacker. Darker red shading indicates higher support for retaliation. For example, 29% of respondents recommended retaliating against India in cases where authorities were 60% certain that they were responsible for an initial attack. All other conjoint attributes are held even.

At the lowest end of the spectrum, where certainty about the identity of the attacker is a mere 10%, we observe minute support for retaliation across the board. At this level of certainty, the predicted support for retaliating against China is a meagre 16 percentage points, while support for striking the United Kingdom is a similarly low 14 percentage points. The span between these two

extremes is barely 2 percentage points. Yet when authorities convey higher (yet not absolute) confidence in their assessments, a diverging pattern begins to manifest. Once attributional confidence reaches 70%, for example, support for retaliating against China rises to 42 percent, while support for targeting the United Kingdom remains relatively low at 24 per cent. The differential in support has increased from 2 percentage points at low confidence levels, to a mammoth 18 percentage points at high confidence levels. At these levels of confidence, the perceived plausibility of an attack by rivals such as Russia and China seems to lead people to overlook equivocal evaluations of certainty. Yet for allies such as the UK and Israel, the implausibility of such an attack causes people to assess the uncertainty differently and use it an excuse to 'dismiss the charges.'

Put simply, perceptions of countries as adversaries or allies affect the way in which fluctuating certainty levels matter for the predicted probability that someone will choose retaliation. This is most true at boundaries between implicit categories of low, medium and high confidence discussed above, where the public may be seeking more information to determine how to decide liminal cases. Historical allies, such as the United Kingdom, possess a reservoir of good will that blunts the effect of increasing certainty once it passes the 50 percent level. Adversaries such as China do not. In this way, cyber uncertainty can hinder public support for conflict, depending on the way that the uncertainty interacts with pre-existing geopolitical realities.

Even though the public generally holds consistent attitudes towards foreign countries (Castano, Bonacossa & Gries, 2016), foreign policy views are increasingly split according to domestic partisan identities (Mirilovic & Kim, 2017). We must therefore account for potential partisan divisions in understanding how attributional uncertainty interacts with people's views of countries as friends or foes (H4). In Figure 4, we present the same certainty by country interaction results from Figure 3, this time disaggregated by partisan alignment.[5]

[5] Non-aligned individuals and political independents are analyzed as a third-sub-group in Online Appendix C.

Figure 4: Certainty and country interactions – disaggregated by party identification

	Democrats					Republicans				
Attributional Certainty ↓	China	Russia	India	Israel	UK	China	Russia	India	Israel	UK
90	51%	48%	45%	48%	46%	59%	54%	51%	43%	40%
80	48%	45%	35%	45%	34%	51%	42%	42%	33%	36%
70	43%	44%	39%	33%	31%	47%	48%	24%	24%	24%
60	35%	35%	37%	30%	31%	41%	31%	32%	18%	26%
50	30%	31%	17%	18%	21%	34%	22%	26%	18%	13%
40	21%	25%	19%	23%	21%	24%	19%	12%	14%	10%
30	22%	23%	14%	20%	14%	28%	18%	9%	15%	10%
20	23%	21%	22%	11%	16%	23%	18%	11%	8%	8%
10	20%	14%	15%	18%	19%	11%	14%	10%	12%	5%
Mean: 60 – 90	44%	43%	39%	39%	35%	49%	44%	37%	29%	31%
Mean: 10 – 50	23%	23%	18%	18%	18%	24%	18%	14%	13%	9%

Note: Cells indicate the percentage likelihood of support for retaliation at every level of uncertainty for each suspected attacker. Darker red shading indicates higher support for retaliation. Additional analyses assessing the statistical significance of the difference between Democrats and Republicans appears in Online Appendix D.

The results indicate that how uncertainty elicits higher and lower support for retaliation towards certain countries is heavily contingent on political ideology. Republicans' perception of a country as an ally or rival is a highly influential signal, while Democrats are less sensitive to the identity of the suspected attacker. As a result, Democrats are less willing to retaliate against adversaries, and more willing to retaliate against allies than Republicans. Looking at Figure 4, for Democrats, the average difference in support for retaliating against China and the UK at all levels of uncertainty is 7 percentage points - with slightly higher support for launching action against China. Yet for Republicans, the average difference in support for striking China and the UK across all levels of certainty is 16 percentage points - more than double that of Democrats. Republicans, it seems, give more benefit of the doubt to allies, and are quicker to jump to worst-case conclusions if rivals are in the picture.

This ideological interaction effect is stronger than other heterogeneous factors such as digital literacy and education – both of which are significant predictor of attitudes following cyberattacks (Kostyuk & Wayne, 2021). The minimal role played by literacy, news consumption and education (discussed in Online Appendix E) further highlights the importance of partisan identity in interpreting uncertainty.

Our final interaction analysis focuses on a second schema that we hypothesized to play a role during uncertain cyberattacks – the mode of retaliation (H5). We anticipated that respondents would exhibit high relative support for cyber-retaliation over conventional retaliation when the identity of the attacker is not completely known. In Figure 5 we present the interaction between attributional certainty and mode of retaliation.

Figure 5: Certainty and retaliation mode interactions

Attributional Certainty ↓	Naming and Shaming	Economic Sanctions	Cyber Attack	Conventional Military Attack	Difference in Support Between Cyber and Conventional Attacks
90	54%	46%	42%	38%	4%
80	47%	39%	36%	34%	2%
70	40%	34%	29%	27%	3%
60	37%	28%	27%	26%	1%
50	21%	22%	20%	22%	-2%
40	21%	18%	18%	15%	3%
30	19%	17%	15%	14%	2%
20	15%	15%	15%	14%	1%
10	14%	14%	15%	13%	2%
Mean: 60 – 90	44%	37%	34%	31%	3%
Mean: 10 – 50	18%	17%	17%	16%	1%

Note: Cells indicate the percentage likelihood of support for retaliation at every level of uncertainty for each mode of retaliation. Darker red shading indicates higher support for retaliation. All other attack attributes are held even.

What jumps out immediately is a consistently low willingness to retaliate across all modes of retaliation when certainty is at 50% and below. We had expected that at low levels of attributional certainty, the public would 'hedge their bets' by exhibiting a preference for less violent retaliation that would avoid escalatory behavior. But this preference does not manifest. Rather, when authorities are uncertain about the identity of the attacker, people equally spurn violent and non-violent retaliatory actions (all weapons are equally ineffective against an unknown enemy). Yet where there is higher confidence about who is responsible for an attack – between 60% and 90% – retaliation becomes more palatable. Our fifth hypothesis is therefore partially verified.

Discussion

The ambiguity surrounding cyberattacks has typically been discussed as an operational and strategic concern. In this paper, we lower the focus of attention to the human level, and show that cyber uncertainty powerfully shapes preference formation in the aftermath of attacks. Uncertainty is a core and unavoidable facet of cyberspace (Dunn Cavelty, Eriksen & Scharte, 2023). While it is futile to attempt to overcome uncertainty, its effects can be understood, measured, and incorporated into our thinking about cyber threats. To examine the effect of uncertainty, we proposed and tested an uncertainty threshold mechanism using a nationally representative sample of 2,025 U.S. respondents who were exposed to various cyberattacks for which authorities expressed differing levels of certainty about the identity of the responsible party. While lower certainty in attribution is associated with less support for retaliation, we find that this mechanism is contingent on the suspected identity of the attacker. Diplomatic allies possess a reservoir of good-will that blunts the effect of uncertainty, while

strikes against rivals are accepted in the face of far lower levels of certainty. This is explained by the fact that uncertainty encourages the use of cognitive schemas that causes people to fall back upon cues that confirm pre-existing belief, such as the image of the suspected country. This finding marries classical theories of public opinion in foreign policy with a new cyber reality and bears important implications for the field of international relations.

First, leaders should pay careful attention to public attitudes when considering retaliatory action following cyberattacks. The current findings clarify how much certainty is needed for the public to support retaliation against an aggressor nation. To the extent elites think like the public (Kertzer, 2022) or public attitudes shape foreign and defense policy decisions (Tomz & Weeks, 2013), the findings suggest that the certainty of blame assignment can influence geostrategic policy outcomes. This mechanism works in two directions – offensively and counter-offensively. From an offensive perspective, when planning cyber operations, military officials have a small yet crucial amount of flexibility in terms of leaving traces that can be ascribed back to the source of the attack. Contrary to popular accounts, cyberattack can never be fully anonymous since analyses of attribution incorporates technical and geo-political factors (Rid & Buchanan, 2015). Yet so long as overall confidence in ascribing a name to the source of the attack remains at 50% or below, officials can avoid added public pressure that would be placed on rivals to retaliate. From a counter-offensive point of view, authorities will need to swiftly formulate high-confidence projections about who is responsible for an attack, at 60% certainty or higher, to accrue public support for retaliatory strikes. To be clear, we are not arguing that the tail can wag the dog, and that public opinion can override strategic doctrine and compel leaders to retaliate. Rather, we emphasize that public opinion is an important factor that is undoubtedly part of the decision-making calculus considered by leaders.

Second, people compensate for the uncertainty of cyberspace by adopting images about countries as friends or foes, which guide their reasoning about world affairs. This particular mental shortcut manifests as a diplomatic good-will / aversion effect. If authorities are not entirely certain about who is responsible for an attack, and the alleged aggressor is an ally, the ambiguity will cause people to fall back on their view of the country as a friend, forestalling public support for retaliation. Counter-intuitively, this finding may encourage the ongoing use of cyber espionage among allies, since they can draw on a reservoir of good will to avoid reprisals so long as there remains at least some uncertainty about their responsibility. With cyber espionage norms still in flux (Libicki, 2017), our findings offer evidence about the interaction between alliances and uncertainty in cyberspace. Uncertainty, however, is less of a shield for countries perceived as adversaries. It has been customarily assumed that countries can leverage digital uncertainty to attack rivals so long as they maintain a veneer of doubt about whether they are truly responsible. We show that this expectation is unwarranted, and that the public will still support retaliation so long as it abides by their pre-existing view of the attacker as a rival. The fact that such viewpoints are guided to a large extent by partisan identification, offers a new way in which domestic partisanship intervenes in foreign policy attitudes.

Last, our findings add valuable nuance to an ongoing debate about public support for cyber strikes. Past research maintains that the general public enthusiastically support the use of cyberattacks due to its low cost, limited destructiveness, and ability to avoid friendly and civilian casualties. However, we show that the public preference for employing cyber tools is not absolute. Had the public perceived cyber weaponry as a fully anonymous and non-escalatory tactic, then we would have seen strong support for its deployment even at low to moderate levels of attributional certainty. Yet this wasn't the case, indicating the public has developed a keen understanding of the significance of cyberattacks following a string of highly destructive incidents. We learn from this that the public preference for cyberattacks does exist, yet only when certain conditions for military action are in place.

We underline a crucial proviso of any discussion about uncertainty. What is uncertain today, need not be tomorrow. When it comes to emerging technologies that carry with them the power to shock and awe, long-term exposure "mitigates the emotional response associated with it, normalizing novel threats over time" (Gomez & Whyte, 2021: 1137). According to this view, the effect of uncertainty on public opinion may wane over time as the public becomes more acquainted with cyberspace and cyberattacks. Nevertheless, a decade of observational, experimental and physiological evidence of psychological distress stemming from cyberattacks (Shandler, Gross & Canetti, 2023), along with persistent media depictions of exaggerated cyber doom narratives (Bastug, Onat & Guler, 2023; Makridis, Maschmeyer and Smeets, 2023), suggest that public trepidation surrounding cyberspace will endure for some time to come.

As a concluding note, the conspicuous absence of destructive cyberattacks has reinforced the idea that cyberattacks are used predominantly as a tool of sub-crisis manoeuvring allowing states to operate below the threshold of armed conflict (Maschmeyer, 2023a; Harknett & Smeets, 2022; Kostyuk & Gartzke, 2022). This may be the case, yet what is more important from the public's vantage point is not the objective reality of cyberattacks, but how the attacks are construed in the media. It is not uncommon for accidental digital mishaps to be hyperbolically reported as major cyberattacks (see for example Teale (2023) on the Florida water plant, where the sensational hack turned out, several years later, to be an employee mistake). At the time, leaders had to endure significant public pressure to respond to the alleged attack, making the question of attributional confidence extremely salient.

In all, this article has contributed to our understanding of how uncertainty in cyberspace influences public reactions to cyberattacks. The discrete choice experiment at the heart of the study quantifies how much uncertainty about 'who done it' might inhibit public support for retaliation. The short answer is: uncertainty matters. The long answer reveals that 60% certainty is the threshold that must be achieved in attributional assessments to get the public on side, yet this is contingent on the identity of the purported attacker, and the type of policy response under discussion. Underlying both of these answers is the fact that public opinion matters, and we can now better assess how the uncertainty characteristic of cyberattacks influences the formation of public judgements.

References

Arsenault, Amelia, Sarah Kreps, Keren L.G. Snider & Daphna Canetti (2023) Cyber scares and prophylactic policies: cross-national evidence on the effect of cyber attacks on public support for surveillance. *Journal of Peace Research*.

Backhaus, Sophia, Michael L. Gross, Israel Waismel-Manor, Hagit Cohen & Daphna Canetti (2020) A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking* 23(9): 595-603.

Baram, Gil (2023). A sliding scale of secrecy: toward a better understanding of the role of publicity in offensive cyber operations. *Journal of Cyber Policy* 7(3): 275-293.

Bastug, Mehmet F., Ismail Onat & Ahmet Guler (2023) Threat construction and framing of cyberterrorism in the US news media. *International Journal of Cybersecurity Intelligence & Cybercrime* 6(1): 29-44.

Berinsky, Adam J. (2009) *In time of war: Understanding American public opinion from World War II to Iraq*. University of Chicago Press.

Blagden, David (2020) Deterring cyber coercion: the exaggerated problem of attribution. *Survival 62*(1): 131-148.

Boebert, W. Earl (2010). A survey of challenges in attribution. In *Proceedings of a workshop on Deterring CyberAttacks* (pp. 41-54).

Brantly, Aaron F. (2016) *The decision to attack: military and intelligence cyber decision-making* (Vol. 5). University of Georgia Press.

Brewer, Paul R. (2004) Public trust in (or cynicism about) other nations across time. *Political Behavior 26*(4): 317-341.

Brewer, Paul R., Kimberly Gross, Sean Aday & Lars Willnat (2004) International trust and public opinion about world affairs. *American Journal of Political Science* 48(1): 93-109.

Canetti, Daphna, Michael Gross, Israel Waismel-Manor, Asaf Levanon & Hagit Cohen (2017) How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychology, Behavior, and Social Networking* 20(2): 72-77.

Castano, Emanuele, Alain Bonacossa & Peter Gries (2016) National images as integrated schemas: subliminal primes of image attributes shape foreign policy preferences. *Political Psychology* 37(3): 351-366.

Clark, David D. & Susan Landau (2011) Untangling attribution. *Harvard National Security Journal* 2: 323.

Dunn Cavelty, Myriam, Christine Eriksen & Benjamin Scharte (2023) Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research* 26(7): 801-814.

Egloff, Florian J. & Myriam Dunn Cavelty (2021) Attribution and knowledge creation assemblages in cybersecurity politics. *Journal of Cybersecurity 7*(1), tyab002.

Egloff, Florian J. & James Shires (2023) The better angels of our digital nature? Offensive cyber capabilities and state violence. *European Journal of International Security 8*(1): 130-149.

Egloff, Florian J. (2020a) Public attribution of cyber intrusions. *Journal of Cybersecurity 6*(1): tyaa012.

Egloff, Florian J. (2020b) Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy 41*(1): 55-81.

Fazal, Tanisha M. (2021) Life and limb: new estimates of casualty aversion in the United States. *International Studies Quarterly* 65(1): 160-172.

Fischerkeller, Michael P. & Richard J. Harknett (2017) Deterrence is not a credible strategy for cyberspace. *Orbis* 61(3): 381-393.

Gartzke, Eric & Jon R. Lindsay (2015) Weaving tangled webs: offense, defense, and deception in cyberspace. *Security Studies 24*(2): 316-348.

Gelpi, Christopher, Peter D. Feaver & Jason Reifler (2009). *Paying the human costs of war: American public opinion and casualties in military conflicts*. Princeton University Press.

Gomez, Miguel A. (2021) Overcoming uncertainty in cyberspace: strategic culture and cognitive schemas. *Defence Studies 21*(1): 25-46.

Gomez, Miguel A. (2019) Past behavior and future judgements: seizing and freezing in response to cyber operations. *Journal of Cybersecurity 5*(1): tyz012.

Gomez, Miguel A. & Chris Whyte (2021) Breaking the myth of cyber doom: securitization and normalization of novel threats." *International Studies Quarterly 65(4): 1137-1150.*.

Gross, Michael L., Daphna Canetti & Dana R. Vashdi (2016) The psychological effects of cyber-terrorism. *Bulletin of the Atomic Scientists 72*(5): 284-291.

Gross, Michael L., Daphna Canetti & Dana R. Vashdi (2017) Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity 3*(1): 49-58.

Hainmueller, Jens & Daniel J. Hopkins (2015) The hidden American immigration consensus: A conjoint analysis of attitudes toward immigrants. *American Journal of Political Science* 59(3): 529-548.

Hainmueller, Jens, Daniel J. Hopkins & Teppei Yamamoto (2014) Causal inference in conjoint analysis: Understanding multidimensional choices via stated preference experiments. *Political Analysis* 22(1): 1-30.

Hansel, Mischa (2018) Cyber-attacks and psychological IR perspectives: explaining misperceptions and escalation risks. *Journal of International Relations and Development 21*(3): 523-551.

Harknett, Richard J. & Max Smeets (2022) Cyber campaigns and strategic outcomes. *Journal of Strategic Studies* 45(4): 534-567.

Healey, Jason & Robert Jervis (2020) The escalation inversion and other oddities of situational cyber stability. *Texas National Security Review* (Fall 2020).

Hedgecock, Kathryn & Lauren Sukin (2022) Responding to uncertainty: the importance of covertness in support for retaliation to cyber and kinetic attacks. *Journal of Conflict Resolution*: 00220027231153580.

Ivie, Robert L. & Oscar Giner (2009) More good, less evil: Contesting the mythos of national insecurity in the 2008 presidential primaries. *Rhetoric & Public Affairs* 12(2): 279-301.

Kertzer, Joshua D (2022) Re-assessing elite-public gaps in political behavior. *American Journal of Political Science* 66(3): 539-553.

Koblentz, Gregory D. & Jonathan B. Tucker (2010) Tracing an attack: the promise and pitfalls of microbial forensics. *Survival* 52(1): 159-186.

Kostyuk, Nadiya & Erik Gartzke (2022) Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine. *Texas National Security Review* (Summer 2022).

Kostyuk, Nadiya & Carly Wayne (2021) The microfoundations of state cybersecurity: cyber risk perceptions and the mass public. *Journal of Global Security Studies* 6(2): ogz077.

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.

Leal, Marcelo M. & Paul Musgrave (2023) Hitting back or holding back in cyberspace: experimental evidence regarding Americans' responses to cyberattacks. *Conflict Management and Peace Science 40*(1): 42-64.

Libicki, Martin (2017) The coming of cyber espionage norms. In *2017 9th International Conference on Cyber Conflict (CyCon)*, pp. 1-17. IEEE.

Libicki, Martin C. & Olesya Tkacheva (2020) Cyberspace escalation: ladders or lattices?. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*: 60.

Lin, Herb S. (2016) Attribution of malicious cyber incidents: from soup to nuts. *Journal of International Affairs* 70(1): 75–137.

Lin-Greenberg, Eric (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 R. (2015) Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity 1*(1): 53-67.

Loewenstein, George & Ted O'Donoghue (2007) The heat of the moment: modeling interactions between affect and deliberation. *Unpublished manuscript*: 1-69.

Lupovici, Amir (2016) The "Attribution Problem" and the social construction of "Violence": taking cyber deterrence literature a step forward. *International Studies Perspectives* 17(3): 322-342.

Makridis, Christos, Lennart Maschmeyer & Max Smeets (2023) If it bleeps it leads? - media coverage on cyber conflict and misperception". *Journal of Peace Research*.

Maschmeyer, Lennart (2021) The subversive trilemma: why cyber operations fall short of expectations. *International Security 46*(2): 51-90.

Maschmeyer, Lennart (2023a) Subversion, cyber operations, and reverse structural power in world politics. *European Journal of International Relations 29*(1): 79-103.

Maschmeyer, Lennart (2023b) A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies 46*(3): 570-594..

Maurer, Tim (2018) *Cyber mercenaries : the state, hackers, and power*. Cambridge University Press.

McDermott, Rose (2019) Some emotional considerations in cyber conflict. *Journal of Cyber Policy 4*(3): 309-325.

Mirilovic, Nikola & Myunghee Kim (2017) Ideology and threat perceptions: American public opinion toward China and Iran. *Political Studies* 65(1): 179-198.

Peters, Ellen, Daniel Västfjäll, Paul Slovic, C. K. Mertz, Ketti Mazzocco & Stephan Dickert (2006) Numeracy and decision making. *Psychological Science* 17(5): 407-413.

Rid, Thomas & Ben Buchanan (2015) Attributing cyber attacks. *Journal of Strategic Studies 38*(1-2): 4-37.

Rovner, Joshua (2019) Cyber war as an intelligence contest. *War on the Rocks*, *16*.

Schneider, Jacquelyn, Benjamin Schechter & Rachael Shaffer (2022) A lot of cyber fizzle but not a lot of bang: evidence about the use of cyber operations from wargames. *Journal of Global Security Studies* 7(2): ogac005.

Sevenans, Julie (2021) How public opinion information changes politicians' opinions and behavior. *Political Behavior 43*(4): 1801-1823.

Shandler, Ryan, Michael L. Gross & Daphna Canetti (2021) A fragile public preference for cyber strikes: evidence from survey experiments in the United States, United Kingdom, and Israel. *Contemporary Security Policy 42*(2): 135-162.

Shandler, Ryan, Michael L. Gross, Sophia Backhaus & Daphna Canetti (2022) Cyber terrorism and public support for retaliation–a multi-country survey experiment. *British Journal of Political Science 52*(2): 850-868.

Shandler, Ryan, Keren L. G. Snider & Daphna Canetti (2022) The Political Psychology of Cyberterrorism. In D. Osborne & C. Sibley (Eds.), *The Cambridge Handbook of Political Psychology*, Cambridge University Press.

Shandler, Ryan, Michael L. Gross & Daphna Canetti (2023) Cyberattacks, psychological distress, and military escalation: an internal meta-analysis. *Journal of Global Security Studies 8*(1): ogac042.

Shandler, Ryan, Nadiya Kostyuk & Harry Oppenheimer (2023) Public opinion and cyberterrorism. *Public Opinion Quarterly* 87(1): 92 – 119.

Shandler, Ryan & Miguel A. Gomez (2023) The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology & Politics* 20(4): 359-374.

Shandler, Ryan & Daphna Canetti (2023) Special issue introduction: cyber-conflict - moving from speculation to investigation. *Journal of Peace Research*.

Sniderman, Paul M. (2018) Some advances in the design of survey experiments. *Annual Review of Political Science 21*: 259-275.

Snider, Keren L, Ryan Shandler, Shay Zandani & Daphna Canetti (2021) Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity 7*(1): tyab019.

Teale, Chris (2023) Florida city water cyber incident allegedly caused by employee error. *Government Computer News*. https://gcn.com/about/?oref=gcn-nav.

Tomz, Michael, Jessica L. Weeks & Keren Yarhi-Milo (2020) Public opinion and decisions about military force in democracies. *International Organization 74*(1): 119-143.

Tomz, Michael R. & Jessica L. Weeks (2013) Public opinion and the democratic peace. *American Political Science Review 107*(4): 849-865.

Valeriano, Brandon & Ben Jensen (2022) De-escalation pathways and disruptive technology. *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, 64.