Journal of Global Security Studies, 8(1), 2023, 1–19
https://doi.org/10.1093/jogss/ogac042
Research Article

Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis

Ryan Shandler [1], Michael L. Gross [2], and Daphna Canetti [2]

[1]University of Oxford, UK and [2]University of Haifa, Israel

Abstract

To what extent can cyberattacks wreak havoc and terrorize modern society? Until now, this question has revolved around the potential of cyber operations to cause physical destruction or other material harm. In this paper, we propose a broader interpretation. We submit that assessing cyberthreats through the prism of physical destruction has obscured the human dimension of the threat. Instead, we propose calculating the gravity of cyberattacks by measuring *psychological distress*. This approach recognizes that even seemingly inconsequential cyberattacks can levy tremendous damage by traumatizing civilians, undermining societal cohesion, and exacerbating cycles of violence. To test whether cyberattacks cause significant individual harm, we employ an internal meta-analysis looking at eighteen studies conducted in three countries over 6 years. Across these studies, we exposed 6,020 respondents to simulated cyberattacks and conventional attacks. We conclude that cyberattacks can cause high levels of psychological harm—equal even to that caused by conventional political violence and terrorism. This finding overturns a widely accepted view that cyberattacks are a mere irritant at best and a threat to information security at worst. Through this lens, the findings suggest that even nonphysically destructive cyberattacks can trigger consequences that constitute a legally defined armed attack that permits using armed force in self-defense. We conclude by discussing how the onset of psychological distress generates political pressure in support of retaliation and can lead to military escalation.

Résumé

¿Hasta qué punto pueden los ciberataques causar estragos y aterrorizar a la sociedad moderna? Hasta ahora, esta pregunta giraba en torno al potencial de las operaciones cibernéticas para causar destrucción física u otros daños materiales. En este artículo proponemos una interpretación más amplia. Sostenemos que evaluar las ciberamenazas a través del prisma de la destrucción física ha oscurecido la dimensión humana de la amenaza. En su lugar, proponemos calcular la gravedad de los ciberataques mediante la medición del malestar psicológico. Este enfoque reconoce que incluso los ciberataques aparentemente insignificantes pueden causar enormes daños al traumatizar a la población civil, socavar la cohesión social y exacerbar los ciclos de violencia. Con el fin de comprobar si los ciberataques causan daños individuales significativos, empleamos un metaanálisis interno que analiza 18 estudios realizados en 3 países a lo largo de 6 años. En estos estudios, expusimos a 6477 encuestados a ataques simulados, tanto cibernéticos como convencionales. Concluimos que los ciberataques pueden causar altos niveles de daño psicológico, iguales incluso a los causados por la violencia política convencional y el terrorismo. Esta conclusión contradice la opinión ampliamente aceptada de que los ciberataques son, en el mejor de los casos, una mera molestia y, en el peor, una amenaza para la seguridad de la información. Desde este punto de vista, los resultados sugieren que

Shandler, Ryan et al. (2023) Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogac042

incluso los ciberataques no destructivos físicamente pueden desencadenar consecuencias que constituyan un ataque armado definido legalmente que permite el uso de la fuerza armada en defensa propia. Concluimos con un análisis de cómo la aparición del malestar psicológico genera presión política en apoyo de las represalias y puede provocar una escalada militar.

Resumen

Dans quelle mesure les cyberattaques peuvent-elles causer des ravages et terroriser la société moderne ? Jusqu'ici, cette question s'est concentrée sur la capacité des cyberopérations d'engendrer une destruction physique ou d'autres dommages matériels. Dans cet article, nous proposons une interprétation plus large. Nous avançons que l'analyse des cyberattaques à travers le prisme de la destruction physique a masqué les dimensions humaines de la menace. Nous proposons plutôt de calculer la gravité des cyberattaques en mesurant la détresse psychologique. Cette approche reconnaît le fait que même les cyberattaques en apparence sans conséquences peuvent engendrer des dommages psychologiques considérables en traumatisant les civils, en remettant en cause la cohésion sociale et en aggravant les cycles de violence. Pour vérifier que les cyberattaques sont à l'origine de préjudices personnels importants, nous avons recours à une méta-analyse interne qui s'intéresse à 18 études menées dans 3 pays sur 6 ans. À travers ces études, nous exposons 6 477 participants à des simulations de cyberattaques et d'attaques traditionnelles. Nous concluons que les cyberattaques peuvent entraîner de hauts niveaux de dommages psychologiques. Ces niveaux peuvent même égaler ceux causés par les violences politiques traditionnelles et le terrorisme. Cette observation invalide le point de vue généralement accepté selon lequel les cyberattaques agacent dans les meilleurs cas et dans les pires, constituent une menace pour la sécurité de l'information. Sous cet angle, les conclusions suggèrent que même les cyberattaques non destructrices peuvent s'accompagner de conséquences définies légalement comme une attaque armée justifiant de l'usage de l'armée pour se défendre. Nous concluons en nous intéressant aux façons dont les premiers signes de détresse psychologique génèrent une pression politique pour soutenir les représailles et peuvent aboutir à une escalade militaire.

Keywords: cyberattacks, cyber-conflict, psychological distress, emotional distress, internal meta-analysis, exposure to terrorism

Palabras clave: Ciberataques, conflicto cibernético, malestar psicológico, malestar emocional, metaanálisis interno, exposición al terrorismo

Mots clés: cyberattaques, cyberconflit, détresse psychologique, détresse émotionnelle, méta-analyse interne, exposition au terrorisme

Introduction

Predictions of cyber power upending the world order and transforming the nature of modern warfare have not eventuated, raising the question: can cyberattacks generate strategic consequences and wreak havoc on modern society? Before we abandon the notion of cyber-conflict as a strategic game changer, there is a threat vector that has escaped our collective gaze. If we look beyond the first-order consequences of cyber-conflict—the attempts to steal data, degrade functionality, pilfer funds, or spread misinformation—the hidden threat of the attacks is that they can arouse severe psychological distress. Calculating the gravity of cyberattacks via the metric of psychological distress recognizes that even nonphysically destructive cyberattacks can still inflict tremendous damage by traumatizing civilians, triggering profound psychological harm, undermining human security, and exacerbating cycles of violence. As a result, this paper makes the case that even if most individual attacks may be relatively inconsequential, the cumulative mass of attacks can cause major societal, political, and legal consequences.

In recent years, a series of high-profile cyberattacks have riveted the world. The attacks targeted critical physical infrastructure (the Colonial Pipeline attack that froze gas distributions), critical digital infrastructure (the SolarWinds attack granting hackers access to US

government networks), hospitals and healthcare services, and commercial industries (lucrative ransomware attacks). The sequence and sophistication of these attacks garnered extensive headlines. However, they failed to live up to the exaggerated rhetoric about society's vulnerability to digital intrusions, and the incidents did not resemble the dystopian end-of-times warned about by cyber doomsday proponents. And yet, if we look beyond the lack of enduring physical consequences, these attacks were far more severe than they appeared. As a result of the attacks, members of the public registered a steep decline in public confidence in their governments' ability to defend them against harm (Shandler and Gomez 2022). Meanwhile, millions of people exhibited intense anxiety at their newly perceived vulnerability to attack, prompting calls for stricter cybersecurity policies and encouraging a willingness to sacrifice digital civil liberties for the sake of security (Snider et al. 2021).

In this paper, we suggest that the foremost threat of cyberattacks is not necessarily their first-order consequences—such as the degradation of physical systems, data theft, or loss of access. While these outcomes remain a cause for concern, the fixation on direct effects obscures the more insidious consequences of long-term psychological harm and societal damage. This perspective acknowledges the human dimension of cyberattacks that target individual well-being, morale, and vulnerability. For many cyber perpetrators, ranging from terrorists to state-sponsored hackers and criminal organizations, the primary objective of attacks is to evoke anxiety and terror, and disseminate misinformation among the public. In other words, these are nonphysical aims whose efficacy cannot be simply measured by weighing rubble, counting bodies, or tallying lost funds. Viewing a ransomware attack on a hospital network as minor or unsuccessful, simply because it caused minimal physical destruction and failed to attain a ransom, ignores the extensive psychological and societal damage it can leave in its wake (Shandler and Gomez 2022). Through this lens, the severity of cyber-threats can and should also be measured by the level of psychological distress. We remove from the definition of distress transient or minor emotional responses such as unease or discomfort, and focus our attention on acute psychological distress, including visceral anxiety, enduring anger, and heightened threat perception (Canetti 2017; Byrne et al. 2022).

Currently, there is no consensus whether cyberattacks cause sufficient individual-level harm to constitute a grave threat. Some argue that the bulk of cyberattacks constitute only minor irritants (Lindsay 2013; Gartzke and Lindsay 2015), while other researchers insist that even low-level cyberattacks can levy severe psychological and political consequences (Gross, Canetti, and Vashdi 2016; Canetti et al. 2017). Addressing this dilemma, this paper employs an internal meta-analysis that reviews a series of experimental studies simulating exposure to cyberattacks. An internal meta-analysis is a powerful analytical tool that aggregates and analyzes a pooled collection of experiments conducted by a single researcher or group of researchers. This technique allows us to exploit heightened statistical power to provide precise statistical estimates of treatment effects, and incorporate studies conducted with different population groups at different points of time. We analyze the full gamut of studies conducted by the authors—including null and unpublished findings—to provide accurate, transparent, and conclusive evidence about the individual-level consequences of exposure to cyberattacks. In all, we aggregate and meta-analyze findings from eighteen experimental studies conducted between 2015 and 2021. Over the course of these studies, we exposed 6,020 unique respondents in three countries to simulated cyberattacks and conventional attacks, before measuring the psychological distress that ensued. All studies mimicked how people are exposed to real-world cyberattacks, while maintaining strict ethical standards to ensure participants' well-being.

Our aggregate findings confirm that *cyberattacks cause equally high levels of psychological distress as conventional terrorism and political violence*. This finding challenges international and domestic security norms and practices in several ways. First, psychological suffering elicited by cyberattacks might now be sufficient to constitute an armed attack as defined by international law. If this were the case, cyberattacks could trigger the right of armed self-defense in response to attacks that until now have been perceived as limited strikes. At the same time, the newly perceptible psychological harms of cyberconflict may weigh on calculations of proportionality and so constrain cyber operations. Second, we consider how the extreme psychological distress experienced by the public creates a groundswell of support for military retaliation, thus generating a political tailwind in support of escalation. In this way, we unveil an indirect route by which cyber operations influence foreign policy decision-making.

The Evolution of Cyber-Threats: From Menacing to Exaggerated

Many assessments of cyber-threats allude to a puzzling conundrum. For all the foreboding surrounding cyberattacks, we are yet to see a wave of destructive digital incidents that match the alarmist proclamations

of cyber-doom. In evaluating the scope of cyber-threats, the literature appears to have settled somewhere between the extremities of cyber-doom and cyber-irrelevance. In the paragraphs below, we review how assessments of the scope and nature of cyber-threats evolved from a cyber-Armageddon school of thought to a cyber-skepticism school of thought and, finally, settled on a middle ground.

The first approach to evaluating cyberattacks was known as the *cyber-apocalyptic perspective*. This title was bestowed since much of the early work on cyber-threats depicted individual hackers capable of disrupting critical infrastructure and levying tremendous damage by typing a few simple commands into a computer terminal (Lewis 2002). This apocalyptic view of cyberspace was promoted by prominent advocates such as former CIA Director and US Secretary of Defense, Leon Panetta, who famously predicted that the world was "facing the possibility of a 'cyber-Pearl Harbor' [that] could dismantle the nation's power grid, transportation system, financial networks and government" (Bumiller and Shanker 2012). This view of cyber-threats was widely accepted by a credulous public with limited expertise in cyber matters and no reason to doubt the alarming predictions. Recent polls indicate that much of the public still views cyberterrorism as the single greatest threat to national security (Brenan 2021).

In hindsight, this frightening vision never reflected reality, awakening a backlash and birthing a *cyber-skeptical viewpoint*. Railing against exaggerated predictions of cyberattacks, Thomas Rid famously declared that "cyber war will not take place" (Rid 2013). Rid explained that contrary to earlier hyperbolic claims, cyberattacks had not revolutionized the field of political violence and were merely sophisticated versions of sabotage against which countries knew how to defend. Rid was supported by Cavelty (2010), Valeriano and Maness (2015), and Denning (2009). All agreed that even if terrorists wanted to take advantage of the digital domain, they would encounter significant technical and financial challenges. Beyond the technical and financial constraints, Gartzke explained that cyberattacks are "poorly suited to the task of fomenting terror" (Gartzke 2013, 65). Over time, scholars partly retreated from this extreme renunciation of cyber-threats, asserting that even if cyberattacks do not form a standalone threat, they can still augment modern warfare by facilitating psychological attacks, misinformation, and espionage (Valeriano, Maness, and Jensen 2017).

If the earliest predictions were overstated, and the subsequent viewpoints constituted a more conservative backlash, then it makes sense that a third middle-ground approach has emerged. To this viewpoint, we attach a moniker coined by Jacquelyn Schneider—the *termite infestation perspective*. According to Schneider (2021), the current cyber-threat falls short of cyber pearl harbor but is more than a mere irritant because the accumulation of frequent minor attacks coalesces into a potent hazard. From this perspective, the threat posed by cyberattacks can be viewed as "a termite infestation, eating at the very foundations of our increasingly digital societies" (Schneider 2021). This perspective does not deny that rare and destructive cyberattacks may still eventuate, only that these constitute exceptional circumstances. Rather, the more salient cyber-threats are the minor attacks propagating extensively. If one large attack can harm hundreds or even thousands of victims, the preponderance of individually inconsequential cyberattacks circulating through an interconnected web can traumatize millions of civilians. Beginning from this vantage point, in the sections below, we assess the level of individual psychological harm that attacks of this sort can cause.

Psychological Distress, Violence, and Cyberspace

To understand how exposure to political violence triggers psychological distress, we can draw on rich literatures in political psychology and criminology that have comprehensively studied the psychological effects of violence. In the aftermath of violent incidents, people experience strong psychological reactions that manifest as emotional distress and impaired mental health (Sinclair and Antonius 2013; Albertson and Gadarian 2015; Slone and Mann 2016; Canetti 2017). At one end of the spectrum, exposure to violence can trigger post-traumatic stress disorder (PTSD). PTSD is a debilitating emotional injury that develops when witnessing or experiencing threatening events that elicit fear, helplessness, and horror. Often associated with war veterans, PTSD is frequently identified among victims of crime, political violence, and terrorism in the United States (Galea et al. 2002), Europe (Miguel-Tobal et al. 2006), Israel (Bleich, Gelkopf, and Solomon 2003; Palmieri et al. 2008), and elsewhere. While most studies of violence focus on the death count following terror attacks, the long-term trauma following violent incidents can likewise cripple people's lives and haunt communities long after the rubble has been cleared (Kienzler 2008).

While PTSD is an extreme reaction to life-threatening events, milder psychological distress can still evoke grave consequences (Canetti et al. 2010). Exposure to violence may trigger anxiety (Huddy et al. 2021), anger (Zeitzoff 2014), and heightened perceptions of threat

(Hirsch-Hoefler et al. 2016; Kupatadze and Zeitzoff 2021). These collective negative reactions can be termed "psychological distress" (Canetti-Nisim et al. 2009; Canetti 2017). The onset of psychological distress is consequential for several reasons. Negative emotional responses to terrorism can cause substantial harm to people's lives. Psychological distress is associated with heightened alcohol abuse, depression, and psychosocial and economic resource loss (Hobfoll, Tracy, and Galea 2006; Schiff et al. 2006). Terrorists aim to elicit distress among civilian populations because it can undermine social cohesion, destroy political trust in government institutions, and promote dissatisfaction with government policies. The psychological distress elicited by exposure to terrorism and political violence fosters support for hardline and militant policies (Bleich, Gelkopf, and Solomon 2003; Godefroidt 2022), undermines people's sense of security (Huddy et al. 2005), leads to increased demands for strong military action (Canetti et al. 2021), and diminishes empathy and increases hostility toward minority groups (Canetti et al. 2009).

Extending the Theories to Digital Violence

Do cyberattacks trigger psychological distress in the same manner as conventional violence? It would be reasonable to expect that many of these traditional models and outcomes will apply in the aftermath of cyberattacks since digital violence is simply a methodological subset of a broader category of violence. However, research has identified qualities unique to cyberspace that amplify the subsequent level of psychological harm. First, we note that cyberspace is an almost unfathomably complex domain of operation. Complexity is not an inherently problematic property, yet it raises several dilemmas. The confusion stemming from the novelty and uncertainty of cyberspace likely means that emotions such as anxiety and fear are likely to drive public responses (McDermott 2019). Civilians in prolonged conflict grow accustomed to political violence such as rocket fire since the effects are constrained and well known (Nussio 2020). Nevertheless, cyberattacks are an unknown quality that might trigger emotional responses beyond what the facts of an attack warrant. Indeed, nascent research has suggested that people exhibit heightened fear following cyberattacks due to a sense of helplessness in the face of overwhelmingly complex systems (Kostyuk and Wayne 2021). Other research has shown how dread (the apprehension of uncertain but impending catastrophic harm) in the face of cyberattacks is heightened among those with low domain expertise (Gomez and Villar 2018).

A second intrinsic and influential characteristic of cyberspace is its universal interconnectivity. The development of the Internet of things means that digital connections encroach into people's homes and their very persons. The effect of this explosion of connectivity—both in pure numbers and in terms of its reach into newly connected spaces—means that people are becoming vulnerable to more and new cyberattacks. Furthermore, a consequence of pervasive digital interconnectivity is that cyberspace in general, and cyberattacks in particular, transcend sovereign borders opening the door to hostile, trans-border mischief. Cyber actions taken by actors in one corner of the world can instantaneously target multiple actors in different countries simultaneously. The ubiquity of digital connections and the transnational reliance on common systems that underpin the digital architecture mean that the public may constantly feel threatened.

The third feature of cyberattacks that may alter levels of psychological distress is the difficulty of identifying who is responsible for an attack. The technologically driven nature of cyber intrusions conducted from the other side of the world means that identifying the attacker is far more complex than otherwise (Egloff 2020). The lack of certainty about the identity of a cyber-attacker can amplify perceptions about the extent of the risk (Kaminska 2021). Cyber-attackers have attained an aura of omniscience since they can launch attacks from any corner of the world without warning (Cavelty 2012). Suppose civilians believe that governments and security authorities cannot identify cyber-attackers who consequently operate in an environment of impunity. In that case, attributional uncertainty can influence the public perception of the scope and nature of the cyber-threat (Shandler, Kostyuk, and Oppenheimer 2023).[1]

Collectively, these features of cyberspace—the complexity, universal interconnectivity, and attributional ambiguity—are likely to aggravate the emotional consequences experienced by victims of cyberattacks. Even if cyberattacks do not cause the same physical destruction as conventional violence, we expect these exacerbating qualities to evoke negative emotional responses beyond what is warranted by the facts of an attack. Therefore, we hypothesize that exposure to cyberattacks will cause mental suffering and psychological distress on par with conventional attacks.

1 We note that in contrast to this view, Gartzke (2013) has suggested that the lack of attribution may leave the public perplexed rather than terrorized, which would mitigate the negative effects of attributional ambiguity.

Methodology: An Internal Meta-Analysis

How much psychological distress must an attack cause to be considered serious? In the absence of any objective threshold of "significant" psychological distress, we utilize a comparative perspective. Specifically, we compare the psychological harm caused by exposure to cyberattacks with the harm caused by exposure to conventional kinetic violence. We focus on this comparison since it is universally accepted that conventional political violence and terrorism can elicit severe distress and trauma. Therefore, if cyberattacks trigger the same level of distress, we can conclude that the extent of the harm is meaningful.

To carry out this analysis, we employ an internal meta-analysis. Internal meta-analyses are similar to conventional meta-analyses in that they combine and meta-analyze the results of multiple scientific studies addressing the same research question. The key difference is that internal meta-analyses confine the population of included studies to those conducted by a single researcher.[2] Although this technique is common in psychology and other disciplines, it is still relatively rare in the political sciences.[3] We use this technique since, at present, the majority of experimental projects that expose respondents to simulated cyber violence have emerged from a single research group. Appendix A in the online supplementary files details the results of an extensive literature review conducted to verify the paucity of experimental research in the field of cyber-conflict.

A meta-analytical approach is particularly worthwhile when searching for a null finding. In this case, we hypothesize that there is no significant difference in the level of distress caused by conventional and cyber incidents. Traditional inferential statistics struggle to validate null hypotheses without unrealistically large sample sizes. Yet, if the cumulative evidence of a meta-analysis supports a nonsignificant outcome, then this constitutes persuasive evidence (Goh, Hall, and Rosenthal 2016). By combining numerous studies, the technique can succinctly summarize findings across studies and present far more precise estimates.

Another noteworthy benefit offered by internal meta-analyses is that it promotes transparency by alleviating the problems of "file drawering" and "p-hacking." The first of these failings refers to the practice of publishing only statistically significant findings, and leaving null findings to gather dust in file drawers. The second failing, known as p-hacking, refers to the practice of arbitrarily altering statistical models in search of positive significance scores. Internal meta-analyses in general, and our study in particular, combat these problems by broadly including *all* pilot and non-published studies, thus avoiding the distorting effect of a publication bias (Goh, Hall, and Rosenthal 2016).[4]

The inclusion criteria for our meta-analysis require that (1) studies be experimental in nature (i.e., the treatments were randomly assigned by the researcher) and (2) studies include a cyber-attack condition and an equivalent conventional attack treatment condition where all aspects of the treatment groups are identical apart from the method of attack. Following best practices, all results from all studies were included regardless of the sample size, the statistical significance of the findings, or the publication status. To be clear, in our main analysis, exposure to conventional incidents acts as the control condition against which cyberattacks are compared. Later in this article, we rerun the analysis, replacing the control condition with a classical neutral control group who were not exposed to any attacks, to test the robustness of the results.

The meta-analysis dataset consists of eighteen experiments fielded across eight different studies. The first study in the dataset was published in 2015, and the most recent were unpublished working papers in 2021. The various experiments were fielded in three countries (the United States, the United Kingdom, and Israel). They included diverse adult samples (either nonstudent convenience samples provided by companies such as Amazon Mechanical Turk or local or national public samples). The sample sizes range from $N = 42$ up to $N = 500$, with a combined total of 6,020 unique respondents. A complete list of studies is given in table 1.

We used Cochrane Risk of Bias 2 measure (RoB-2) to evaluate the methodological rigor of each study (Sterne et al. 2019). The bias assessment technique evaluates studies by examining potential biases in the randomization process, deviations from intended interventions, missing outcome data, outcome measurements, and

2 Or in this case, a single team of researchers.

3 For an example of a political science article employing an internal meta-analysis, see Clifford, Sheagley, and Piston's (2021) article in the *American Political Science Review*. See also Schuler, Ivanov, and Wänke (2017) and Urbanska, Perhson, and Turner (2019).

4 Furthermore, the included studies report very different results. Several studies have shown that exposure to cyberattacks elicits higher levels of anxiety and threat perception than those triggered by conventional violence. Others find that exposure to cyber violence results in the same or lower levels of psychological distress. As such, this minimizes the concern of p-hacking, since findings were not artificially manipulated to produce a particular result.

Table 1. Overview of experimental studies

Study no	Publication	Type of cyberattack	Year	Sample size	Country	Outcome variable(s) measured	Description of manipulation
1	Gross, Canetti, and Vashdi (2016)	Cyberterror attacks	2016	784	Israel	Anxiety, threat perception	Video news report describing a cyberattack on national water purification network
2	Backhaus et al. (2020)	Cyberterror attacks	2019	231	United States, England, Israel	Anxiety, anger, threat perception	Video news report describing a cyberattack on national water purification network
3	Shandler, Gross, and Canetti (2021)	Cyberterror attacks	2020	734	United States, England, Israel	Anxiety, anger	Video news reports about cyberattacks against transportation infrastructure
4	Shandler et al. (2022)	Cyberterror attacks	2018	2,078	United States, England, Israel	Anxiety, anger, threat perception	Video news reports about cyberattacks against transportation infrastructure
5	Snider et al. (2022a)	Cyberattacks	2021	630	United States, England, Israel	Anxiety, anger, threat perception	Video news reports about cyberattacks against transportation infrastructure
6	Snider et al. (2022b)	Cyberterror attacks	2021	118	Israel	Threat perception	Virtual reality simulation of a cyberattack against railway networks
7	Gross, Canetti, and Vashdi (2017)	Cyberattacks	2016	684	Israel	Anxiety, threat perception	Video clip depicting cyberattacks on critical infrastructure
8	Snider et al. (2021)	Cyberattacks	2015	761	Israel	Threat perception	Video news reports about various attacks

selective reporting. Independent researchers rated each included study using the RoB-2 scale. The complete analysis (appendix B in the online supplementary files) finds that the study is at low risk of bias across all domains.

The included studies utilize various experimental methods that creatively simulate exposure to cyber and conventional violence. In many studies, participants viewed vivid, professionally produced television news reports depicting cyberattacks against critical infrastructure such as rail networks, water purification plants, or electric grids. Breaking news reports comprise an ecologically valid manipulation that tends to be more authentic than vignettes or other fabricated treatments. Moreover, news reports and social media are the key pathways through which the public learns about security incidents. Other studies in this dataset utilized virtual reality treatments that immersed participants within 360° virtual environments where they directly experienced catastrophic and deadly attacks on critical infrastructure.

In addition, the studies include a variety of types of cyberattacks by focusing on cyberterrorism, cyberwarfare, or other cyberattacks by unknown perpetrators. The rationale is to heighten the authenticity of the experimental treatments by utilizing a variety of realistic cases. Likewise, the experimental treatments refer to lethal and nonlethal attacks against national infrastructures, the theft and dissemination of sensitive information, and breaches of military systems. To ensure that our analyses shed light on the type of attack, and not the outcome of attack, we only include studies that expose participants to equivalent cyber and conventional outcomes. That is, if the conventional violence treatments led to fatalities, then the cyber treatment must have caused the exact same outcome. Likewise, if the cyber experimental treatment caused only nonlethal effects, the same effects must have appeared in the conventional treatment group.

For the dependent variable, we operationalize "psychological distress" as an amalgamation of anxiety, anger, and perceived threat (Ross 2011). These variables were measured in several ways—ranging from self-reported survey questions to analyses of salivary cortisol as a physiological measure of stress. To assess measurement biases, we pool only the self-reported survey data since these utilized identical scales applied consistently across all studies.

Anxiety centers on the uncertainty and unpredictability of a threat and is defined as a future-oriented emotional state characterized by feelings of apprehension and the arousal of the autonomic nervous system (Grupe and Nitschke 2013). We measured anxiety using the short-form Spielberger State-Anxiety Inventory-6 (Marteau and Bekker 1992). This commonly used measure incorporates six items that quantify state (extrinsic) and trait (intrinsic) anxiety. *Anger* is "an emotional state that consists of feelings that vary in intensity, from mild irritation or annoyance to intense fury and rage" (Spielberger, Reheiser, and Sydeman 1995). We measured anger using the shortened version of the widely used State-Trait Anger Expression Inventory (Spielberger 1988). This measure possesses four items that assess the intensity of anger at a particular time. Last, *threat perception* is a cognitive appraisal of the danger posed by a class of threat, such as cyberattacks (Hirsch-Hoefler et al. 2016). As perceptions of threat rise, they undermine personal and collective security. Threat perception was gauged using a five-item measure that tested the level of respondents' concern about the possibility of threats to their security (Huddy et al. 2002).

Results

As a guiding analytical strategy, we employed a random-effects meta-analysis model because, unlike fixed models, this technique does not assume that there is one "true" effect size. Furthermore, random-effects models better contend with between-study heterogeneity, thus providing more accurate and generalizable effect size estimates (Lipsey and Wilson 2001). To reiterate our analytical structure, our effect size of interest is a Cohen's d between cyberattacks and conventional attacks. In other words, the conventional incidents act as our control condition, against which cyberattacks are compared. This allows us to determine whether cyberattacks cause substantially different outcomes than the control condition of conventional attacks. The meta-analysis results are visualized in figure 1. Each study appears as a separate line, with country-level data disaggregated as separate studies.

Overall, the meta-analysis revealed a nonsignificant main effect, thus corroborating our primary hypothesis that cyberattacks elicit the same level of psychological distress as conventional attacks ($N = 16$, $d = -0.07$, 95 percent confidence interval [CI] = [−0.14, 0.00]). Figure 1 depicts several individual studies in which cyberattacks trigger less psychological distress than conventional attacks (these studies possess a negative standardized mean difference and skew to the left side of the y-axis). Likewise, several studies show that the opposite is true, and cyberattacks cause greater psychological distress. However, most of the effects are nonsignificant. When combined with a nonsignificant Q ($p < 0.57$) and low I_2 (0 percent), we can glean that there is low heterogeneity among the included studies and

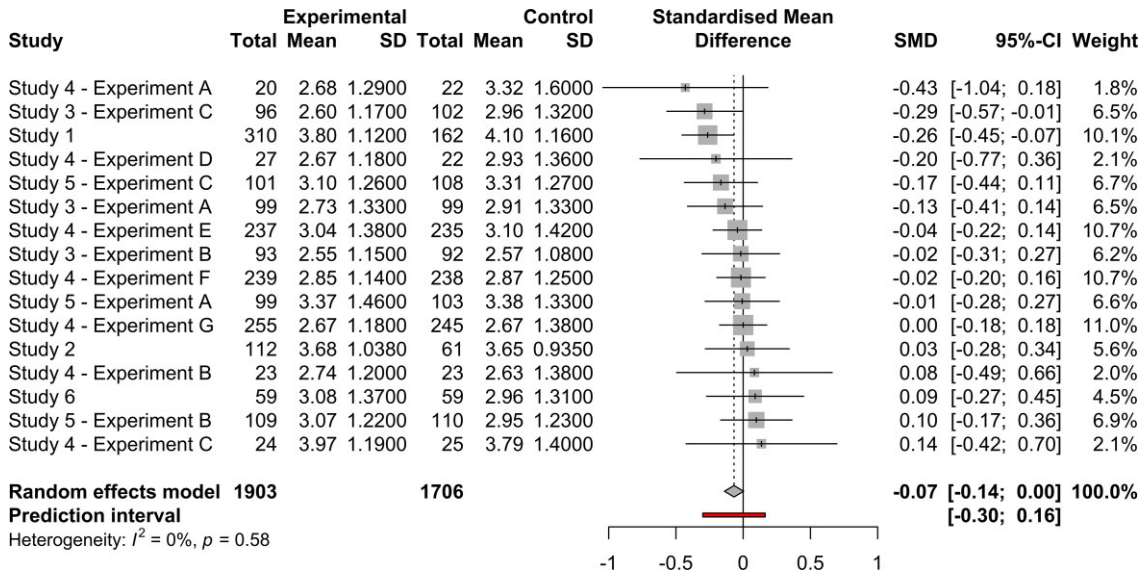

Figure 1. Forest plot comparing the effect of exposure to cyberattacks and conventional attacks on psychological distress. *Note*: Positive effects indicate that cyberattacks cause greater psychological distress than conventional attacks, and vice versa. We report for each included study the sample size, means, and standard deviations for each of the treatment groups. We further report Fisher's *z* value, and the corresponding 95 percent CIs. Effect sizes are illustrated with squares whose sizes reflect the relative weight of each study in the random-effects meta-analysis. The diamond depicts the overall effect size of the meta-analytic estimate and its 95 percent CI.

that they all reflect the same underlying effect.[5] Therefore, weighing the cumulative evidence of our studies, the combined research can conclude that cyber and conventional violence leads to the same high level of psychological distress. While traditional inferential statistical analyses cannot confidently validate such a null hypothesis, the combined evidence of a meta-analysis with small CIs and a nonsignificant total effect size leads us to confidently conclude that the overall effect is zero.

In operationalizing psychological distress, we follow the literature in amalgamating several constituent variables. While this combination may be theoretically sound, it behooves us to demonstrate no statistical dependence between the effect sizes for each emotion. The risk, in this case, is two-fold. First, the same respondents may register support for multiple dependent elements. Second, we run the risk of a systematic error since all data emanated from a single lab with uniform between-study measurement techniques. Put otherwise, the benefit of an internal meta-analysis can magnify the risk of researcher error. To account for this, we conduct a robust variance estimate (RVE) meta-analysis, which extracts each element and analyzes it as though it is a standalone variable. The full RVE plot in figure 2 disaggregates the constitutive elements of psychological distress (anxiety, anger, and threat perception) as they appear in each included study. The effect size weight is shown for each of the forty-two outcome measures arranged by study. Larger black boxes represent larger weights in the meta-analysis, and bars represent 95 percent CIs.

The aggregated RVE effect size specifies an overall effect size of $g = -0.09$ (p = n.s.). This result upholds our primary findings by showing an insignificant main effect, thus confirming that the inclusion of particular psychological responses does not sway the results. A low amount of between-study heterogeneity was observed in the analysis (I^2 = 30.84 percent, $\tau^2 = 0.01$).[6] This and the fact that the vast majority of studies possessed CIs overlapping with zero indicate that the RVE-aggregated effect was not driven by specific outcome measures.

Finally, while our data demonstrate that exposure attacks to cyberattacks elicit the same level of distress as exposure to conventional attacks, this does not attest to the significance of the distress. Civilians grow accustomed to certain types of expected violence (Nussio 2020). So, it may be that exposure to both conventional and cyberattacks elicits identical levels of distress—neither of which is distinguishable from zero. As such, we run a secondary

5 Cochran's Q and I^2 are test statistics that evaluate the consistency of a meta-analytic effect.

6 τ^2 denotes the variance of effect size parameters across the population of studies.

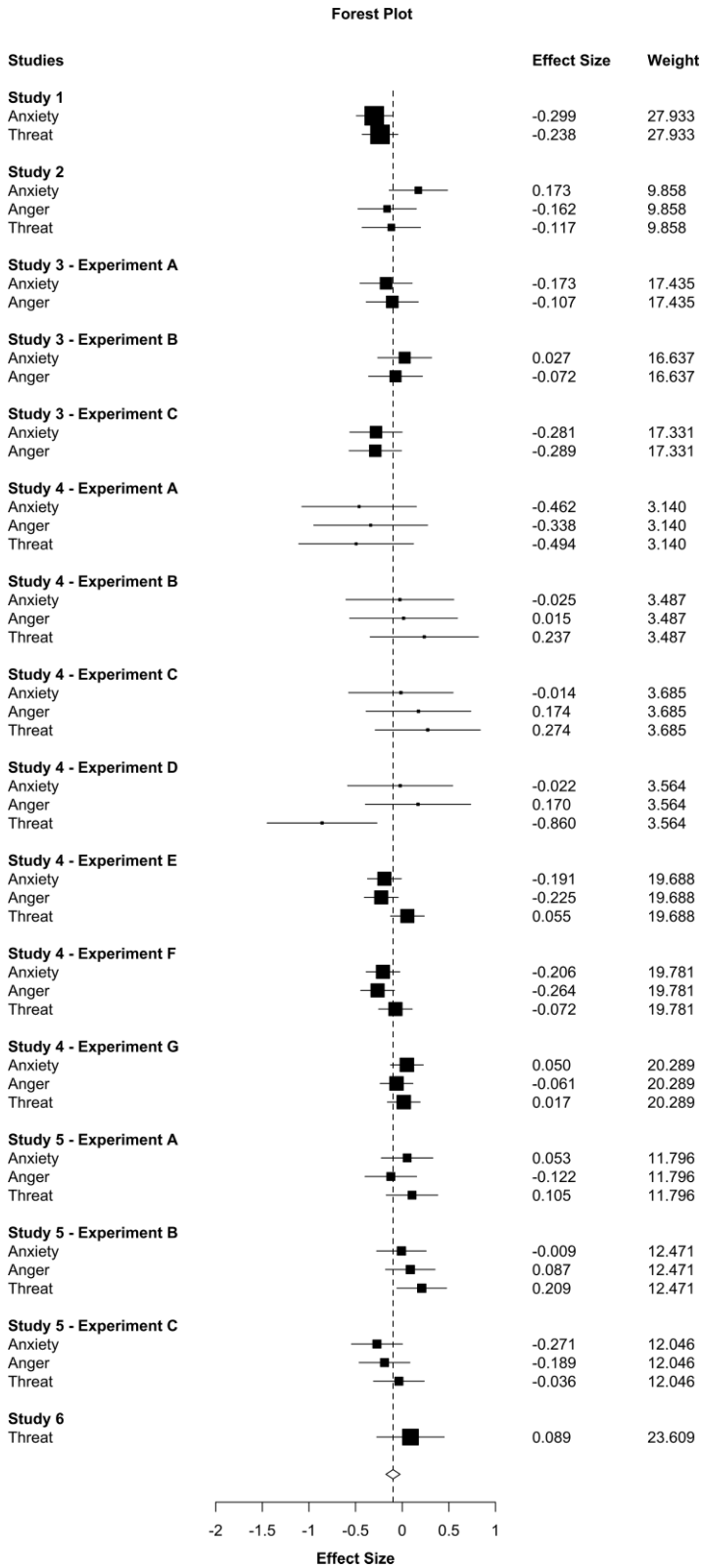

Figure 2. Robust variance estimation forest plot, correlated effects model. *Note*: Positive effects indicate that cyberattacks cause greater psychological distress than conventional attacks, and vice versa. Effect sizes are illustrated with squares whose sizes reflect the relative weight of each study in the RVE meta-analysis. Lines indicate 95 percent CIs. The diamond depicts the overall effect size of the RVE meta-analytic estimate.

meta-analysis that compares the psychological distress triggered by exposure to cyberattacks as opposed to a control group that was not exposed to any form of violence. The full forest plot appears in appendix C in the online supplementary files. The results confirm that belonging in the treatment group, in this case exposure to cyberattacks, is associated with a significant and large increase in psychological distress ($N = 14$, $d = 0.70$, 95 percent CI = [0.39, 1.00]).

Robustness Tests: Refuting an Alternative Explanation

There remains an alternative interpretation of our data. Could the observed null effect not be caused by the difficulty in simulating conventional violence in controlled experimental settings? If this were the case, the equal levels of distress measured in the aftermath of conventional and cyberattacks may result from our inability to evoke the full extent of the terror experienced following nondigital acts of violence. This possibility is largely refuted by our previous analysis, which demonstrated that participants in conventional violence treatments experienced significantly more distress than those control group participants who received no treatments. Nonetheless, the analysis does not entirely preclude the possibility that our cyber treatments were more effective at tapping into a deeper and more authentic emotional harm.

To forestall this possibility, we conduct a series of subgroup analyses. If our findings were a function of experimental realism, then we would expect to find different results when we look at particular subgroups. For example, video depictions of violence may be more effective at generating distress than newspaper or virtual reality stimuli. Likewise, residents of certain countries may be more susceptible to the treatments than others. In all, we run three separate subgroup analyses that test whether our null finding is sensitive to (1) the country where the experiment took place, (2) the experimental method, and (3) publication status (whether or not the results were published in scientific journals).

The tests of subgroup differences conclusively indicate that our findings are robust to country, experimental type, and publication status. Our null-effect finding does not exist as a result of the inability of certain manipulation types to evoke distress, the prominence of the null effect in any particular country, nor due to a bias of publicizing only corroborating results. If our main finding were indeed a function of the difficulty of generating distress in certain conditions, we would have expected that certain categories of experiments were more potent at generating the full extent of distress. The full results of the subgroup analyses appear in online appendix D.

In addition to these data-driven robustness tests, we are further reassured by a preponderance of external observational evidence that corroborates our findings. According to a 2021 Gallup study, American survey respondents ranked cyber-threats as the most critical threat facing the nation—more even than Russian militarism, COVID, or the development of nuclear weapons by Iran (Brenan 2021). This fearful view of cyberattacks—where they are consistently ranked as being just as terrifying (or more than) as international terrorism, the spread of infectious diseases, Chinese military power, North Korean nuclear weapons, and other threats—has recurred consistently in survey data over many years (Mccarthy 2016; Norma 2018; Sheth 2019). These observational data add credence to our findings and suggest that our conclusions are not a matter of modest experimental capacity.

Discussion

Cyber discourse has long been characterized by fears of catastrophic cyberattacks that have not transpired. To many researchers and policymakers, the absence of any destructive cyberattacks signified that the threat was overblown. We claim to the contrary: cyberattacks have been measured with an imperfect metric that highlights physical destruction at the expense of psychological harm. To quantify the extent of the psychological consequences stemming from cyberattacks, we report the results of an internal meta-analysis encompassing 6,477 unique respondents from three countries, drawn from eighteen individual studies conducted over six years. The data demonstrate that cyberattacks arouse equally high levels of psychological distress as conventional warfare—an outcome fraught with far-reaching consequences.

Our results overturn a widely accepted view that cyberattacks are a mere irritant at best and a threat to information security at worst. If this were the end of the story, then this alone would demand a recalibration of our thinking about national security threats. Understanding that cyberattacks can wreak havoc and

precipitate lingering harm, even if they do not cause explosive damage to critical infrastructure, demands a rethinking of how we measure and respond to such threats. Yet, looking upon these results from the perspective of international security, our findings suggest that psychologically harmful cyberattacks may surpass the threshold of an armed attack, with all of the military, legal, and ethical implications that ensue. Second, we sketch an indirect pathway, according to which the psychological distress suffered by the public dramatically shifts public opinion on military escalation, generates political pressure in support of retaliation, and so influences the course and conduct of international relations.

Psychologically Harmful Cyber Operations as Sufficiently Severe Armed Attacks

Facing attack, nations must ask two critical legal questions as they formulate their response. First, does the attack cause sufficient death, injury, and destruction to constitute an "armed" attack that gives states the right to respond with armed force in self-defense? Second, is an armed response appropriate and proportionate (Cannizzaro 2006; Kretzmer 2013)? Appropriate in this context means "necessary," in that only armed force and no other less harmful course of action will successfully repel aggression. Proportionality is trickier. When a state is attacked, it may be enough to choose the least harmful means to defend itself successfully irrespective of subsequent casualties. Or, it may be the case that states must also refrain from military operations that cause excessive harm. Much depends upon what self-defense hopes to accomplish. One may concede, for example, the necessity of responding with sustained military campaigns to meet armed attacks by Argentina in 1982 and Hezbollah in 2006, but nonetheless conclude that each response was disproportionate in what were essentially wars of choice. Seeking only to maintain sovereignty or strengthen deterrence, neither Britain nor Israel could justify each war's human and material costs. In contrast, existential wars of self-defense in places such as Kuwait or Ukraine may be accompanied by widespread devastation that is both necessary and proportionate.

Comprising "territorial intrusions, human casualties or considerable destruction of property" (Dinstein 2001), the human and material costs of war are the key metric for recognizing armed attacks and assessing proportionate, self-defensive responses. Although keyed to kinetic warfare, the same logic and law of self-defense governs cyberwarfare no less than conventional warfare. Considering a nation's right to respond with force to an armed attack under Article 51 of the United Nations (UN) Charter, The Tallinn Manual on the International Law Applicable to Cyber Operations (henceforth the Tallinn Manual) agrees that "a cyber operation that seriously injures or kills a number of people or that causes significant damage to, or destruction of, property would satisfy the scale and effect requirements [of armed attacks]" and "establish a right of self-defense" against state and non-state actors (Schmitt 2017, 341).

However, cyberattacks rarely, if ever, cause loss of life or major physical destruction. If physical consequences were all that mattered, cyberattacks would never cause sufficient death or devastation to push the attack across the threshold of an armed attack and, thereby, warrant an armed response. Cyber-threats would constitute a legally escalatory dead-end. And, for this reason, cyberspace is often viewed as a non-escalatory military domain (Kreps and Schneider 2019; Lin-Greenberg 2022). Yet, physical destruction is not the only ingredient of legal harm. Critically, the Tallinn experts also understand that severe injuries may be entirely psychological, noting that it is:

> [r]easonable to extend the definition [of attack] to serious illness and *severe mental suffering* that are tantamount to injury. In particular, note that Article 51(2) of Additional Protocol I prohibits "acts or threats of violence the primary purpose of which is to spread terror among the civilian population" (see also Rule 98). Since terror is a psychological condition resulting in mental suffering, inclusion of such suffering in this Rule [defining a cyber-attack] is supportable through analogy." (Schmitt 2017, 417, emphasis added).

In other words, a cyber operation that causes *severe* psychological distress would be tantamount to an armed attack (by a state in relation to Article 51) or terrorism (by a non-state) and thereby trigger the right of self-defense. Similarly, the International Committee of the Red Cross (ICRC) emphasizes the crucial role of severe mental suffering in assessments of proportionality. Psychological, no less than physical, injuries weigh in on civilian casualties and assessment of collateral harm. The ICRC notes:

> There is a general recognition that serious and well-documented forms of *mental harm*, such as post-traumatic stress disorder (PTSD), do have significant and long-term impacts on individuals and are increasingly deemed problematic … To date, international jurisprudence has not considered the role of mental harm in the assessment of incidental injury to the civilian population … In this framework, mental harm has been understood to be more than a "minor or temporary impairment of mental faculties, but it does not

necessarily have to be permanent and irremediable." (Gisel 2016, 34, emphasis added).

Applying these principles to cyberwarfare, we can reformulate the two critical questions confronting nations as they consider the appropriate response to cyber aggression. First, has the cyberattack caused a sufficient degree of harm, in this case psychological harm, to surpass the threshold of an armed attack and warrant an armed response? Second, assuming that the psychological harm is sufficient, how must military planners factor the debilitating psychological sequelae of cyber operations into calculations of proportionality and assessments of collateral damage as they consider their response?

Answering each question requires a clear, operational definition of "severe mental suffering" and "mental harm." When and how are they measured, and by whom? While calculations of death and injury are relatively straightforward, there are few easy metrics to gauge psychological harm. PTSD and other forms of psychological distress are possible criteria. However, they often require sophisticated diagnostic techniques unavailable in conflict areas, and their effects often manifest symptoms over extended periods, confounding timely or causal determinations. More generally, the notion of "severe" or other qualitative descriptions of extreme suffering and harm is common in international humanitarian law but rarely defined rigorously. Indeterminate metrics abound, such as references to torture (*severe* pain and suffering), proportionality *(excessive* loss of life or injury), and inhumane weapons (*superfluous* injury and *unnecessary* suffering). Considering the ravages of war necessary to trigger the right of self-defense, the International Court of Justice fashioned, but did not detail, the widely acknowledged position that only the "most grave" uses of force qualify as an armed attack (Nicar. vs. U.S 1986).

Often wedded to evaluations of physical damage, suffering, and loss of life, attempts to introduce concrete criteria to quantify "severe," "excessive," "most grave," or "unnecessary" harm often fail to gain widespread acceptance (Gross 2008). At the same time, death and injury are not the sole measures of war's ravages. Increasingly, states are called upon to consider the degradation of the environment and destruction of infrastructures that may exacerbate pollution, mortality, and morbidity, even though they are challenging to measure at the point of attack. In every case, policy makers and commanders draw on incomplete information (and sometimes only "gut" feelings) to determine whether an attack and appropriate response have crossed the threshold that regulates the use of force. Introducing psychological harm into this mix is long overdue, but similar challenges bedevil attempts to measure and assess mental suffering during war.

While the data we present here help give equivalence to such critical notions as severe harm, the debate over where the line is drawn will continue. The Tallinn Manual argues that in contrast to PTSD, "inconvenience, irritation, stress or fear … or a decline in civilian morale" do not qualify as collateral damage (Schmitt 2013, 160). The ICRC experts take a slightly different tack, declaring that "inconvenience, stress or fear incidentally caused by attacks are not relevant for an assessment under the principle of proportionality" (Gisel 2016, 35; see also Lawson and Mačák, 2021, 23). However, in neither case do the experts present psychological data to bolster their claim.

In rebuttal, we argue that this view is too narrow and does not account for current research into the effects of war and terror-related mental suffering. Our data suggest that the outcomes dismissed by the Tallinn Manual and ICRC review—fear, stress, and decline in morale—can collectively cause suffering on par with the distress caused by terrorism. Mental health experts and political psychologists recognize that emotional distress need not reach the level of PTSD to cause significant personal and societal harm. In many ways, emotional distress is equally as harmful and threatening as physical harm (Aggarwal and Aggarwal 2015). One result is an evolving conception of terrorism that moves away from bestial terror replete with brutally horrific casualties to terrorism that draws on fear to undermine civil society by depriving the target government of a population capable of rational deliberation (Waldron 2004).

To be clear, our survey experiments do not directly measure whether exposure to cyberattacks elicits psychological distress at sufficiently severe levels to meet the ambiguous thresholds posed in the Tallinn Manual and ICRC guidance. Our findings do, however, provide logical evidence and validated, well-established measures of mental suffering that support the proposition that cyberattacks can cause sufficiently severe psychological distress to activate the relevant clauses pertaining to armed attacks and proportionate responses. First, our data demonstrate that cyberattacks elicit equally significant levels of distress and suffering as conventional attacks. Second, compelling trends in international jurisprudence and legal discussions, as exemplified by the Tallinn and ICRC guidance reports, conclude that severe psychological distress in war is central to evaluations of armed attacks and calculations of proportionality. As a result, we conclude that exposure to cyberattacks can (although will not necessarily) cause sufficiently severe mental suffering to qualify as an armed attack and trigger the right of self-defense. It is no surprise that Albania, for example, recently reacted to 2022 Iranian cyberattacks by threatening to invoke Article 5 of the North Atlantic Treaty to mobilize collective self-defense as permitted in

response to an armed attack (Miller 2022). The Iranian cyberattacks did not cause substantial material harm, but the fact that they shut down access to government websites and services across the country laid the ground for spiking anxiety and failing trust in government institutions.

At the same time, incipient psychological pain and suffering must also inform decisions about the degree of force necessary to repel aggression. Warring parties must factor in the prospect of psychological and physical harm as they plan defensive operations. By folding psychological harm into proportionality, armies may see that some military operations previously considered proportionate (because they did not result in widespread casualties) are nonetheless disproportionate after considering subsequent mental suffering. In this way, attention to psychological distress expands the reach of proportionality and should diminish civilian casualties.

On our reading and pursuant to our data, international norms task political and military authorities with assimilating psychological harm into strategic and tactical decision-making. At the same time, severe mental suffering bears political consequences. The experience of psychological distress can shift public opinion toward foreign policy issues and thereby generate political conditions that encourage an escalatory military response. The subsequent section concentrates on this indirect pathway.

Indirect Effects: Psychologically Harmful Cyber Operations Shifting Public Opinion

To this point, we have viewed severe psychological harm as a conceptual threshold that can ethically and legally justify a military response. However, psychological distress suffered by civilians may also shape foreign policy decision-making. The pathway comprises two stages. First, psychological harm following cyberattacks shifts public opinion. Second, shifts in public opinion influence national decision-making. This pathway is indirect and offers a secondary perspective to consider the political consequences of cyber operations.

The pathway's first leg links psychological harm and public policy preferences. Previously, we discussed how the anxiety and fear associated with political violence arouses a newly arisen perception of the world as a malevolent and dangerous place. As a consequence of their threat-driven emotional reorientation, voters adopt certain policy positions to regain a sense of security. When it comes to cyber-threats, recent empirical research verified that public exposure to cyberattacks leads to substantial shifts in political attitudes (Shandler, Snider, and Canetti 2022). Various studies have shown how exposure to cyberattacks corrodes public trust in government institutions (Gross, Canetti, and Vashdi 2016; Shandler and Gomez 2022), and influences support for intrusive surveillance (Snider et al. 2021). It is clear that the emotional distress associated with cyberattacks generates the conditions for reevaluating core beliefs toward privacy, and that attacks are likely to spawn a realignment of the privacy-security paradigm for the digital age.

Why do cyberattacks have such potent political consequences? Cyberattacks exploit the absence of trustworthy attribution in cyberspace (Kello 2013; Poznansky and Perkoski 2018; Kaminska 2021), the lack of domain expertise among the public (Kostyuk and Wayne 2021), and the dread associated with cyberspace (Gomez and Villar 2018), to shake society's trust in the safety and resilience of digital infrastructure. Believing that government authorities cannot effectively protect against damaging cyberattacks intensifies the public's sense of cyber fatalism wherein omniscient and malicious perpetrators run havoc. It is quite astonishing that despite a singular absence of catastrophic cyber-strikes, more than 82 percent of the American public view cyberterrorism as a critical threat to society—far more than infectious diseases (72 percent), Russian military power (44 percent), or global warming (58 percent) (Brenan 2021). The public fear of cyber-threats is overwhelming, exacerbating the political consequences that follow any attacks.

We draw attention to one particular political outcome of exposure to cyberattacks that is especially pertinent to our enquiry—support for escalation and military retaliation. Widespread distress following cyberattacks elicits incessant public demands for military retaliation (Gross, Canetti, and Vashdi 2017; Shandler, Gross, and Canetti 2021; Shandler et al. 2022; Leal and Musgrave 2023). Even if the identity of the cyber-attacker is unknown, a frequent scenario in cyberspace, public anger still encourages a generalized desire for some kind of military action. If governments previously believed that "merely irritating" cyberattacks would fail to move a "merely irritated" public, this research suggests otherwise. Put simply, even nondestructive cyberattacks trigger substantial psychological harm, leading directly to public demands for a military response to cyber violence.

The mounting public pressure to retaliate following cyberattacks clashes with prevailing norms against cross-domain escalation in cyberspace (Kreps and Schneider 2019; Lin-Greenberg 2022; Valeriano and Jensen 2022). In this way, the de-escalatory nature of cyberconflict may be counteracted by the imposition of extreme public pressure to retaliate, even across domains (Shandler, Gross, and Canetti 2021). In essence, we argue that the escalatory nature of cyber operations is not solely contingent on the technical characteristics of

cyber capabilities, but that dynamics of public opinion must be incorporated into the evermore complex models of cyber-escalation. This dynamic is two-fold. While the previous section explains how cyber violence ignites fears and shifts public opinion, the following describes how public pressure can influence foreign policy decision-making.

There is extensive literature exploring the responsiveness of elected officials but no clear consensus about how they respond to the foreign policy views of their voters. While many scholars are skeptical about the role of public input, most agree that public opinion impacts decisions to engage in military operations to at least some degree (Sobel 2001; Klarevas 2002; Foyle 2004; Lin-Greenberg 2021). For example, Foyle (2004) demonstrated how the American public's appetite for retaliation was a key factor influencing the Bush administration's decision to go to war in Iraq. Political and national security officials are understandably attuned to the views of the public they ostensibly serve, a political truth that extends even outside of democratic nations (Quek and Johnston 2017). An overwhelming public enthusiasm for retaliation following an attack will place considerable pressure on officials to approve military force.

That exposure to political violence brings about public pressure for retaliation is not unique to cyber-conflict. All acts of violence generate psychopolitical reactions. Still, there are reasons to expect that the process by which public opinion influences foreign policy decision-making may play out differently in the cyber realm. First, cyber-threats prompt outsize public panic relative to their actual destructive potential. The exaggerated public fear in the aftermath of cyberattacks is likely to pressure political elites who would otherwise be willing to dismiss many such attacks as de-escalatory behavior (Valeriano and Jensen 2022). Second, cyber-threats are still novel phenomena, and there is a lack of inter- and intra-national consensus about how to respond to such attacks. The lack of policy agreement provides greater room for public input, with elites becoming more willing to follow popular views in these cases (Kreps 2010; Kreps and Das 2017).

While additional research is still needed to empirically verify elite responsiveness to public fears surrounding cyber-threats, there is evidence to conclude that psychological distress following cyberattacks will shift the public's foreign policy attitudes and often pressure national officials to act. Having shown that the onset of psychological distress provides the legal and ethical backing for a military response, we show that it also generates the political conditions that facilitate an escalatory response due to mounting public demands for a vigorous defense.

Conclusion

The emergence of novel cyber-threats challenges many of the theories and norms of international security built for a pre-digital world. Conducting empirical research on the causes and effects of cyber-threats has proven challenging due to swiftly advancing technologies that make findings quickly redundant, a culture of secrecy, and ethical challenges in measuring the effects of violence. This study takes up the challenge of conducting theoretically driven and methodologically rigorous research focusing on human behavior in the context of cyber-conflict (Valeriano 2022). We present the first meta-analysis of a decade's worth of empirical research that exposed more than 6,000 participants in three countries to simulated attacks to measure the ensuing psychological distress.

Using a powerful meta-analytic technique allows us to address a simple question: can cyberattacks cause severe psychological distress? Our findings demonstrate that cyberattacks cause significant psychological harm equivalent to the distress elicited by major terror events. The implications of this finding are manifold. Altering the metric by which we measure the gravity of cyberattacks to account for psychological harm may raise cyberattacks to the level of an armed attack that opens the door to military retaliation. However, the effect is two-edged. Introducing mental suffering into calculations of proportionality and collateral harm also constrains counterattacks and restricts the license to engage armed force—due to both legal analyses and the constraining effect of public opinion on collateral damage (Sagan and Valentino 2020).

Finally, our findings make a significant methodological contribution. Internal meta-analyses are a novel and valuable addition to the methodological toolbox of political science and international relations. Unfortunately, the technique is neglected due to the dearth of empirical studies and the difficulty in acquiring sufficient data to substantiate a meta-analytical inquiry. The absence of meta-analyses is lamentable, since the cumulative evidence offered by a meta-analysis provides more precise, transparent, and rigorous findings that can persuasively resolve discrepancies among smaller studies. Our study demonstrates how meta-analyses, in general, and internal meta-analyses, in particular, can play a role in international security research.

Acknowledgments

The authors gratefully acknowledge the valuable feedback offered by Sophia Backhaus, Amélie Godefroidt, Miguel Gomez, Iris Lavi, and Rose McDermott. The paper benefited greatly from comments offered at a 2021

workshop on the Moral Psychology of War hosted by the Oxford Institute for Ethics, Law, and Armed Conflict. We deeply appreciate the input of the *Journal of Global Security Studies* editorial team and reviewers. Our heartfelt thanks to all members of the Political Psychology Lab who supported the studies reported in this paper.

Funding

This work was supported by the Israel Science Foundation (DC, 594/15; MG, 156/14), the US-Israel Binational Science Foundation (2009460), and the Center for Cyber Law & Policy at the University of Haifa.

Supplementary Information

Supplementary information is available at the *Journal of Global Security Studies* data archive.

References

Aggarwal, Neil K., and Neil Krishan Aggarwal. 2015. *Mental Health in the War on Terror*. Columbia: Columbia University Press.

Albertson, Bethany, and Shana Kushner Gadarian. 2015. *Anxious Politics: Democratic Citizenship in a Threatening World*. Cambridge: Cambridge University Press.

Backhaus, Sophia, Michael L. Gross, Israel Waismel-Manor, Hagit Cohen, and Daphna Canetti. 2020. "A Cyberterrorism Effect? Emotional Reactions to Lethal Attacks on Critical Infrastructure." *Cyberpsychology, Behavior, and Social Networking* 23 (9): 595–603.

Bleich, Avraham, Marc Gelkopf, and Zahava Solomon. 2003. "Exposure to Terrorism, Stress-Related Mental Health Symptoms, and Coping Behaviors among a Nationally Representative Sample in Israel." *JAMA* 290 (5): 612–20.

Brenan, Megan. 2021. "Cyberterrorism Tops List of 11 Potential Threats to U.S." Gallup. Accessed May 9, 2022. https://news.gallup.com/poll/339974/cyberterrorism-tops-list-potential-threats.aspx.

Bumiller, Elisabeth, and Thom Shanker. 2012. "Panetta Warns of Dire Threat Cyberattack on U.S." New York Times, October 11, 2012.

Byrne, Kate G., Yogeeswaran Kumar, Martin J. Dorahy, Jessica Gale, M. Usman Afzali, Joseph Bulbulia, and Chris G. Sibley. 2022. "Psychological Impact of Far-Right Terrorism against Muslim Minorities on National Distress, Community, and Wellbeing." *Scientific Reports* 12 (1): 1–9.

Canetti, Daphna. 2017. "Emotional Distress, Conflict Ideology, and Radicalization." *PS: Political Science & Politics* 50 (4): 940–43.

Canetti, Daphna, Amnon Cavari, Carmit Rapaport, Hadar Shalev, and Stevan E. Hobfoll. 2021. "Individual Exposure to Terror and Political Attitudes: A Physiologically-Based Model of Militancy." *Terrorism and Political Violence* 33 (5): 1055–70.

Canetti, Daphna, Sandro Galea, Brian J. Hall, Robert J. Johnson, Patrick A. Palmieri, and Steven E. Hobfoll. 2010. "Exposure to Prolonged Socio-Political Conflict and the Risk of PTSD and Depression among Palestinians". *Psychiatry: Interpersonal and Biological Processes* 73 (3): 219–31.

Canetti, Daphna, Michael Gross, Israel Waismel-Manor, Asaf Levanon, and 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.

Canetti-Nisim, Daphna, Eran Halperin, Keren Sharvit, and Stevan E. Hobfoll. 2009. "A New Stress-Based Model of Political Extremism: Personal Exposure to Terrorism, Psychological Distress, and Exclusionist Political Attitudes." *Journal of Conflict Resolution* 53 (3): 363–89.

Cannizzaro, E. 2006. "Contextualizing Proportionality: Jus ad bellum and jus in bello in the Lebanese war". *International Review of the Red Cross* 88 (864): 779–92.

Cavelty, Myriam. 2010. The Reality and Future of Cyberwar. CSS Analysis in Security Policy, Zurich, Switzerland.

———. 2012. "The Militarisation of Cyberspace: Why Less May Be Better." 2012 4th International Conference on Cyber Conflict (CYCON 2012), IEEE, 1–13.

Clifford, Scott, Geoffrey Sheagley, and Spencer Piston. 2021. "Increasing Precision Without Altering Treatment Effects: Repeated Measures Designs in Survey Experiments." *American Political Science Review* 115 (3): 1048–65.

Denning, Dorothy E. 2009. "Barriers to Entry: Are They Lower for Cyber Warfare? " *IO Journal* 1 (1): 4.

Dinstein, Yoram. 2001. *War, Aggression and Self-Defence*, 3rd ed. Cambridge: Cambridge University Press.

Egloff, Florian J. 2020. "Public Attribution of Cyber Intrusions." *Journal of Cybersecurity* 6 (1): tyaa012.

Foyle, Douglas C. 2004. "Leading the Public to War? The Influence of American Public Opinion on the Bush Administration's Decision to Go to War in Iraq." *International Journal of Public Opinion Research* 16 (3): 269–94.

Galea, Sandro, Heidi Resnick, Jennifer Ahern, Joel Gold, Michael Bucuvalas, Dean Kilpatrick, Jennifer Stuber, and David Vlahov. 2002. "Posttraumatic Stress Disorder in Manhattan, New York City, after the September 11th Terrorist Attacks." *Journal of Urban Health: Bulletin of the New York Academy of Medicine* 79 (3): 340–53.

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 R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24 (2): 316–48.

Gisel, Laurent. 2016. The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law. In *ICRC International Expert Meeting Report*, June 22–23. https://doi.org/10.1111/ajps.12692.

Godefroidt, Amelie. 2022. "How Terrorism Does (and Does Not) Affect Citizens' Political Attitudes: A Meta-Analysis." *American Journal of Political Science* Forthcoming.

Goh, Jin X., Judith A. Hall, and Robert Rosenthal. 2016. "Mini Meta-Analysis of Your Own Studies: Some Arguments on Why and a Primer on How." *Social and Personality Psychology Compass* 10 (10): 535–49.

Gomez, Miguel A., and Bianca E. Villar. 2018. "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats." *Politics and Governance* 6 (2): 61–72.

Gross, Michael L. 2008. "The Second Lebanon War: The Question of Proportionality and the Prospect of Non-Lethal Warfare." *Journal of Military Ethics* 7 (1): 1–22.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 2016. "The Psychological Effects of Cyber Terrorism." *Bulletin of the Atomic Scientists* 72 (5): 284–91.

———. 2017. "Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes." *Journal of Cybersecurity* 3 (1): 49–58.

Grupe, Dan W., and Jack B. Nitschke. 2013. "Uncertainty and Anticipation in Anxiety: An Integrated Neurobiological and Psychological Perspective." *Nature Reviews Neuroscience* 14 (7): 488–501.

Hirsch-Hoefler, Sivan, Daphna Canetti, Carmit Rapaport, and Stevan E. Hobfoll. 2016. "Conflict Will Harden Your Heart: Exposure to Violence, Psychological Distress, and Peace Barriers in Israel and Palestine." *British Journal of Political Science* 46 (4): 845–59.

Hobfoll, Stevan E., Melissa Tracy, and Sandro Galea. 2006. "The Impact of Resource Loss and Traumatic Growth on Probable PTSD and Depression Following Terrorist Attacks." *Journal of Traumatic Stress* 19 (6): 867–78.

Huddy, Leonie, Stanley Feldman, Theresa Capelos, and Colin Provost. 2002. "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat." *Political Psychology* 23 (3): 485–509.

Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American Journal of Political Science* 49 (3): 593–608.

Huddy, Leonie, Oleg Smirnov, Keren L.G. Snider, and Arie Perliger. 2021. "Anger, Anxiety, and Selective Exposure to Terrorist Violence." *Journal of Conflict Resolution* 65(10): 1764–90.

Kaminska, Monica. 2021. "Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks." *Journal of Cybersecurity* 7 (1): tyab008.

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

Kienzler, Hanna. 2008. "Debating War-Trauma and Post-Traumatic Stress Disorder (PTSD) in an Interdisciplinary Arena." *Social Science & Medicine* 67 (2): 218–27.

Klarevas, Louis. 2002. "The 'Essential Domino' of Military Operations: American Public Opinion and the Use of Force." *International Studies Perspectives* 3 (4): 417–37.

Kostyuk, Nadiya, and Carly Wayne. 2021. "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public." *Journal of Global Security Studies* 6 (2) ogz077. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4122262.

Kreps, Sarah. 2010. "Elite Consensus as a Determinant of Alliance Cohesion: Why Public Opinion Hardly Matters for NATO-Led Operations in Afghanistan." *Foreign policy Analysis* 6 (3): 191–215.

Kreps, Sarah, and Debak Das. 2017. "Warring from the Virtual to the Real: Assessing the Public's Threshold for War over Cyber Security." *Research & Politics* 4 (2): 2053168017715930.

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

Kretzmer, D. 2013. "The Inherent Right to Self-Defence and Proportionality in jus ad bellum". *European Journal of International Law* 24 (1): 235–82.

Kupatadze, Alexander, and Thomas Zeitzoff. 2021. "In the Shadow of Conflict: How Emotions, Threat Perceptions and Victimization Influence Foreign Policy Attitudes." *British Journal of Political Science* 51 (1): 181–202.

Lawson, Ewan, and Kubo Macák. 2021. "Avoiding Civilian Harm From Military Cyber Operations During Armed Conflict". ICRC Expert Meeting, 21–22 January 2020. Geneva: Civilian Harm Report. Accessed December 1, 2022. https://shop.icrc.org/download/ebook?sku=4539/002-ebook.

Leal, Marcelo M., and 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.

Lewis, James A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic & International Studies.

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.

———. 2022. "Evaluating Escalation: Conceptualizing Escalation in an Era of Emerging Military Technologies". *Journal of Politics* Forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4122262

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404.

Lipsey, Mark W., and David B. Wilson. 2001. *Practical Meta-Analysis*. Thousand Oaks, CA: SAGE.

Marteau, Theresa M., and Hilary Bekker. 1992. "The Development of a Six-Item Short-Form of the State Scale of the Spielberger State—Trait Anxiety Inventory (STAI)." *British Journal of Clinical Psychology* 31 (3): 301–6

McCarthy, Justin. 2016. "Americans Cite Cyberterrorism among Top Three Threats to US Gallup". Gallup. Accessed July 10, 2022. https://news.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx.

McDermott, Rose. 2019. "Some Emotional Considerations in Cyber Conflict." *Journal of Cyber Policy* 4 (3): 309–25.

Miguel-Tobal, Juan J., Antonio Cano-Vindel, Hector Gonzalez-Ordi, Iciar Iruarrizaga, Sasha Rudenstine, David Vlahov, and Sandro Galea. 2006. "PTSD and Depression after the Madrid

March 11 Train Bombings." *Journal of Traumatic Stress* 19 (1): 69–80.

Miller, Maggie. 2022. Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack. Politico, October 5, 2022. Accessed October 10, 2022. https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

Nicar. vs. U.S. 1986. "Military and Paramilitary Activities in and against Nicaragua." I.C.J. 14, ¶ 181, June 27, 1986.

Norman, Jim. 2018. "North Korea, Cyberterrorism Top Threats to U.S." Gallup. Accessed May 9, 2022. https://news.gallup.com/poll/228437/north-korea-cyberterrorism-top-threats.aspx.

Nussio, Enzo. 2020. "Attitudinal and Emotional Consequences of Islamist Terrorism: Evidence from the Berlin attack." *Political Psychology* 41 (6): 1151–71.

Palmieri, Patrick A., Daphna Canetti-Nisim, Sandro Galea, Robert J. Johnson, and Stevan E. Hobfoll. 2008. "The Psychological Impact of the Israel–Hezbollah War on Jews and Arabs in Israel: The Impact of Risk and Resilience Factors." *Social Science & Medicine* 67 (8): 1208–16.

Poznansky, Michael, and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3 (4): 402–16.

Quek, Kai, and Alastair Iain Johnston. 2017. "Can China Back Down? Crisis De-Escalation in the Shadow of Popular Opposition." *International Security* 42 (3): 7–36.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Ross, Catherine E. 2011. "Collective Threat, Trust, and the Sense of Personal Control." *Journal of Health and Social Behavior* 52 (3): 287–96.

Sagan, Scott D., and Benjamin A. Valentino. 2020. "Weighing Lives in War: How National Identity Influences American Public Opinion about Foreign Civilian and Compatriot Fatalities." *Journal of Global Security Studies* 5 (1): 25–43.

Schiff, Miriam, Rami Benbenishty, Mary McKay, Ellen DeVoe, Xinhua Liu, and Deborah Hasin. 2006. "Exposure to Terrorism and Israeli Youths' Psychological Distress and Alcohol Use: An Exploratory Study." *American Journal on Addictions* 15 (3): 220–26.

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

———. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schneider, Jacquelyn. 2021. "The Cyber Apocalypse Never Came: Here's What We Got Instead." Politico. Accessed November 1, 2022. https://www.politico.com/news/magazine/2021/07/27/cyber-apocalypse-russia-china-warfare-500787.

Schuler, Johannes, Igor Ivanov, and Michaela Wänke. 2017. "Does Money Change Political Views?–An Investigation of Money Priming and the Preference for Right-Wing Politics." *Journal of Social and Political Psychology* 5 (2): 396–414.

Shandler, Ryan, and Miguel A. Gomez. 2022. "The Hidden Threat of Cyber-Attacks: Undermining Public Confidence in Government". *Journal of Information Technology & Politics*. https://doi.org/10.1080/19331681.2022.2112796.

Shandler, Ryan, Michael L. Gross, Sophia Backhaus, and Daphna Canetti. 2022. "Cyber Terrorism and Public Support for Retaliation: A Multi-Country Survey Experiment." *British Journal of Political Science* 52 (2): 850–68.

Shandler, Ryan, Michael L. Gross, and Daphna Canetti. 2021. "A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in the United States, United Kingdom, and Israel." *Contemporary Security Policy* 42 (2): 135–62.

Shandler, Ryan, Nadiya Kostyuk, and Harry Oppenheimer. 2023. "Public Opinion and Cyber-Terrorism." *Public Opinion Quarterly*. Forthcoming.

Shandler, Ryan, Keren L.G. Snider, and Daphna Canetti. 2022. The Political Psychology of Cyberterrorism. In *The Cambridge Handbook of Political Psychology*, edited by D. Osborne and C. Sibley, 565–81. Cambridge: Cambridge University Press.

Sheth, Shreya. 2019. "America's Top Fears 2019." Chapman University Survey of American Fears Wave 6. Accessed May 10, 2022. https://www.chapman.edu/wilkinson/research-centers/babbie-center/_files/americas-top-fears-2019.pdf.

Sinclair, Samuel J. and Daniel Antonius. 2013. eds. *The Political Psychology of Terrorism Fears*. Oxford: Oxford University Press.

Slone, Michelle, and Shiri Mann. 2016. "Effects of War, Terrorism and Armed Conflict on Young Children: A Systematic Review." *Child Psychiatry & Human Development* 47 (6): 950–65.

Snider, Keren L.G., Ryan Shandler, Shay Zandani, and Daphna Canetti. 2021. "Cyberattacks, Cyber Threats, and Attitudes toward Cybersecurity Policies." *Journal of Cybersecurity* 7 (1): tyab019.

Snider, Keren L.G., Amir Hefetz, Ryan Shandler, and Daphna Canetti. 2022a. "What is it About Cyberattacks that Drives Support for Surveillance Policies? Insights from Experiments in the UK." Working Paper.

Snider, Keren L.G., Amit Cohen, Giulia Dal Bello, Guy Baratz, Béatrice S. Hasler, and Daphna Canetti. 2022b. "Support for Surveillance Hinges on Threat Perception (more than Exposure to Terror)." Working Paper.

Sobel, Richard. 2001. *Impact of Public Opinion on U.S. Foreign Policy since Vietnam*. New York: Oxford University Press.

Spielberger, Charles D. 1988. "Manual for the State-Trait Anger Expression Scale (STAXI)." Psychological Assessment Resources.

Spielberger, Charles D., Eric C. Reheiser, and Sumner J. Sydeman. 1995. "Measuring the Experience, Expression, and Control of Anger." *Issues in Comprehensive Pediatric Nursing* 18 (3): 207–32.

Sterne, Jonathan A.C., Jelena Savović, Matthew J. Page, Roy G. Elbers, Natalie S. Blencowe, Isabelle Boutron, and Christopher J. Cates et al. 2019. "RoB 2: A Revised Tool for Assessing Risk of Bias in Randomised Trials." *BMJ* 366: l4898.

Urbanska, Karolina, Samuel Pehrson, and Rhiannon N. Turner. 2019. "Authority Fairness for All? Intergroup Status and Expectations of Procedural Justice and Resource Distribution." *Journal of Social and Political Psychology* 7 (2): 766–89.

Valeriano, Brandon. 2022. "Why Can't Cyber Scholars Move beyond the Basics?" Cato Institute. Accessed December 1, 2022. https://www.cato.org/commentary/why-cant-cyber-scholars-move-beyond-basics.

Valeriano, Brandon, and Benjamin Jensen. 2022. "De-Escalation Pathways and Disruptive Technology". *Cyber Peace: Charting a Path toward a Sustainable, Stable, and Secure Cyberspace* 64.

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

Valeriano, Brandon, Ryan C. Maness, and Benjamin Jensen. 2017. "Cyberwarfare Has Taken a New Turn: Yes, It's Time to Worry." *Washington Post: The Monkey Cage* 7 (13).

Waldron, Jeremy. 2004. "Terrorism and the Uses of Terror." *The Journal of Ethics* 8 (1): 5–35.

Zeitzoff, Thomas. 2014. "Anger, Exposure to Violence, and Intragroup Conflict: A 'Lab in the Field' Experiment in Southern Israel." *Political Psychology* 35 (3): 309–35.