A FRAGILE PUBLIC PREFERENCE FOR CYBER STRIKES

Evidence from Survey Experiments in the United States, United Kingdom and Israel

Contemporary Security Policy

The Version of Record of this manuscript has been published and is available in Contemporary Security Policy (January 2021) at https://doi.org/10.1080/13523260.2020.1868836

Ryan Shandler[*], Michael L. Gross, & Daphna Canetti

University of Haifa, School of Political Science, Israel

[*] Ryanshandler@gmail.com

The online appendix can be accessed at: https://sites.google.com/view/ryanshandler

Abstract

To what extent does the public support using cyber weapons? We propose that public exposure to the destructive potential of cyber-attacks will dispel the clear cross-national preference for cyber strikes. To test this, we conducted two survey experiments (n = 2,585) that examine support for cyber versus conventional military strikes in the United States, United Kingdom, and Israel. In study 1, we exposed respondents to television news reports depicting various forms of terror attacks, and then measured the subsequent support for retaliatory options. Findings indicate that the high public support for deploying cyber weapons dissipated entirely among respondents exposed to lethal cyber-attacks. In study 2, we probed this vanishing support, finding that exposure to destructive cyber-attacks undercuts the perception of cyber as a less lethal domain, therefore diminishing its appeal. We conclude by discussing how the fragile public preference for cyber weapons encourages military escalation in the short-term.

Keywords: Cyber-attacks; cyber warfare; terrorism; public opinion; foreign policy; cyber escalation.

Introduction

There is a growing debate about the implications of evolving cyber warfare capabilities for the frequency of military conflict. Two clear and competing schools of thought theorize about how cyber warfare will influence the propensity of conflict. The first argument claims that new cyber offensive capabilities allow states to adopt more belligerent policies toward their rivals by making decisions to escalate easier and cheaper. Soldiers need not be deployed or put in harm's way, and the presumed anonymity of cyberspace encourages more risky operations since the source of the attack can be contested. In essence, by offering a strike option that is more publicly palatable, cheaper, anonymous, and less risky to the lives of soldiers, decision makers will be more likely to exercise power and so lower the threshold of warfare (Shandler, 2019; Acton, 2017; Saltzman 2013; Krepinevich, 2012). The counter-argument posits that cyber weapons make interactions less physically violent, thus offering an off-ramp for governments to mitigate potentially explosive situations and avoid the escalatory cycle of war (Valeriano, 2019; Rid, 2013). The plausible deniability associated with cyber-strikes could allow states a way to avoid costly escalation. Moreover, according to this perspective, the relatively low cost of entry to attain cyber capabilities could mean that smaller states and organizations that were previously at a disadvantage against conventionally superior adversaries, can wield a form of deterrence that may reduce the likelihood of war (Liff, 2012). Both sides of this debate have merit. Yet they're both ignoring one critical element: public opinion.

A conspicuously missing element in the debate on how cyber power influences the frequency of conflict is the role of public support for the use of cyber tools in military contexts, and in the fight against terrorism in particular. While there is no agreement about the extent of the influence wielded by the public on matters regarding the use of force, there is broad acceptance that public opinion has at least a measurable impact on the decision to engage in military operations (Foyle, 2004; Klarevas, 2002; Sobel, 2001). Yet the literature on public opinion regarding foreign policy has only recently begun to engage with cyber conflict (Kostyuk & Wayne, 2020; Kreps & Das, 2019; Tomz & Weeks, 2020; Kreps & Schneider, 2019). The slow emergence of research on the public's role in relation to cyber conflict is particularly notable since many of the claims about the utility of cyber warfare implicitly relate to its ability to relieve public pressure on political leaders by reducing the human and economic costs of war. As such, we contend that the level of public support for the use of cyber military power must be taken into account.

To examine the nature of public support for the use of cyber weapons, this article describes two interconnected survey experiments that measure public support for cyber and conventional military retaliatory strikes in three countries (the United States, United Kingdom, and Israel). In the first experiment, we exposed 1,848 respondents to simulated television news reports depicting conventional or cyber terror attacks against critical infrastructure. Respondents were randomly allocated to view one of five experimental conditions (including a control group) that diverged on the form of terrorism (conventional terrorism vs. cyber-terrorism), and the outcome of the attack (lethal vs. non-lethal). After viewing the video news reports, respondents indicated their support for different forms of cyber and conventional military retaliation. Findings reveal that the public supports cyber retaliatory strikes at significantly higher levels than conventional kinetic retaliation (missiles, ground forces, air-strikes). This in itself is not surprising. What is noteworthy is that in all three countries, this strong preference for deploying cyber weapons was entirely absent among one group of respondents—those who were exposed to *lethal* cyber terror attacks. This signifies that cyber options are generally viewed as non-fatal or less hostile military options, and that once this illusion of cyber pacificity is undermined, public support for using cyber weapons diminishes significantly.

The second experiment builds on this foundation by testing *why* public support for cyber retaliation is so much higher than other retaliatory options (and why it disappears following exposure to lethal cyber-attacks). We therefore exposed 737 new respondents in the same three countries to the video manipulations and examined their understandings of the nature of cyber weapons. The findings confirm that public support for the use of cyber weapons is predicated on their perception as a non-lethal military alternative, and that once this perception is dispelled, the public preference for cyber weapons disappears. Together, these studies offer an insight into why civilians exhibit a preference for cyber weapons, and what conditions dispel this preference. We conclude by demonstrating how the shifting public perception of cyber-attacks will initially encourage military escalation—until such time that the public attains an understanding of lethal cyber capabilities—after which the escalatory influence will cease.

Cyber power and the frequency of military conflict

Though the development of cyber warfare capabilities is still at a nascent stage, numerous military and international relations theorists posit that wielding a cyber arsenal will enable additional paths of action in conflict management and may influence leaders' preference for military options over political solutions (Brantly & Smeets, 2020; Saltzman, 2013; Liff, 2012). These slippery slope or cyber-mediated escalation arguments fall into three categories: the realignment of an offensive/defensive balance; risk minimization; and barriers to entry readjustment.

The first argument posits a realignment in the offensive/defensive military balance since cyber weapons ostensibly offer overwhelming offensive benefit, which allows states to adopt more belligerent policies towards their rivals. The offense-defense theory suggests that new military capabilities can influence security dilemmas and affect the likelihood of escalating conflict (Jervis, 1978; Quester, 2002; Van Evera, 2013). According to this view, the lowsignature (hidden attribution) capabilities associated with cyber-attacks, the ubiquitous digital connectedness of critical infrastructure, and the lagging progress of effective cyber-security techniques, tip the military advantage in the direction of attackers (Huntley, 2016; Lieber, 2014; Saltzman, 2013). Since countries can operate in an environment of ambiguity, the likelihood that attacks cannot be wholly attributed to them adds an additional layer of flexibility in planning attacks. Moreover, cyber weapons ease the logistical requirements that have historically decelerated a military escalation and increase the swiftness of conducting military operations (Acton, 2017). Applying this cost-benefit analysis to the deployment of the Stuxnet cyber-attack against Iranian nuclear program, Farwell and Rohozinski (2011) concluded that this offensive recalibration encouraged the exercise of cyber offensive power. While this view is still widely accepted, we acknowledge that several theorists have recently advanced a contrary assessment according to which cyberspace is defense dominant since defenders' influence over the cyber-terrain on their "home turf" offers substantial advantages (Matania & Tal-Shir, 2020; Gartzke & Linsday, 2015).

Second, cyber capabilities allow political actors to minimize the political risks of embarking upon military action by offering a low-cost alternative. Lowering the risks posed to soldiers who need not be placed in harm's way can mitigate the political consequences that often accrue as troops' deaths increase. Additionally, cyber strikes can limit civilian casualties and collateral damage on the enemy side, avoiding international condemnation and lowering the political threshold for the use of force (Acton, 2017).

Third, cyber weapons are both easier to deploy, and can be developed far more cheaply than conventional weapons (Scholz et al., 2018; Eun & Aßmann, 2016). Cyber weapons can therefore "level the playing field" by granting developing countries and non-state actors access to destructive weapons that that are unavailable to them in the conventional realm. Lower barriers to entry open conflict to new actors who did not previously possess the weapons to engage conventionally superior adversaries (Eun & Aßmann, 2016). Cavelty (2010) and Denning (2009) both question the conventional wisdom that low barriers to entry truly exist in the cyber realm because the perception of low barriers of entry relates only to low-level cyber warfare (i.e. denial of service attacks or website defacements). According to their critiques, states looking to use cyber strikes to achieve strategic objectives or as a force-leveling weapon, will encounter the same technical and financial challenges as with conventional weapons since the custom-built software required can cost millions of dollars and take years to develop.

A number of competing theories suggest that the effect of wielding cyber capabilities is more nuanced and is likely to decrease the frequency of conflict, or at least not move the needle substantially in either direction. While cyber weapons may be cheaper to develop and more accessible to minor powers and non-governmental actors, their sustained use would be severely limited in that their effectiveness involves guile, not force (Gombert & Libicki, 2014). Because most cyber-attacks exploit vulnerable computer code, they also reveal system weakness and allow adversaries to employ corrective measures. Following the Stuxnet attack, for example, Siemens and Microsoft quickly patched the zero-day vulnerability that was targeted, thereby negating the future effectiveness of this cyber weapon (Zetter, 2014). As a result, cyber-attacks are likely to be used as a weapon of last resort lest the actors lose access to an expensive and valuable weapon. Such considerations lower the likelihood that cyber capabilities would lead us down the path to conflict.

In this vein, Jensen and Valeriano (2019) suggest that far from intensifying conflict, cyber tools can help de-escalate militarized disputes. In a multi-country experimental war-game scenario, they found that respondents decisively favored using cyber retaliatory strikes as a de-escalating strategy. This outcome mirrored a real-world military skirmish in June 2019 where the Iranian military was reported to have downed an unmanned U.S. surveillance drone (Nakashima, 2019). Signaling restraint, and in the face of significant pressure to respond with overwhelming force, the United States instead chose to de-escalate the situation by conducting covert cyber operations that targeted Iranian missile sites and command and control capabilities (Valeriano & Jensen, 2019). Additional war-game simulations have replicated these findings with a focus on drone technology, suggesting that employing technology that removes warfighters from the frontlines will reduce public demands for escalatory reprisals since any losses would be to remotely operated systems and not to troops (Lin-Greenberg 2019). According to these perspectives, "rather than escalate with conventional military options, cyber operations offer rivals a way to respond to provocations without significantly increasing tension in a crisis" (Valeriano & Jensen, 2019b, p. 6). These conclusions are further mirrored in analyses of recent military conflicts in the Ukraine and Syria, where cyber activities failed to compel discernible battlefield changes (Kostyuk, 2017).

The role of public support in executing military cyber strikes

If we accept the fact that developing cyber technologies can influence the propensity of conflict, what is the role of public support in the use of military force? Traditionally, many assumed that the public was too uninformed to influence debates on such weighty matters as military strikes and foreign policy (Baum & Potter 2015; Small, 1996). Rather, the public's role was simply to elect leaders with the foresight to protect them. In time, however, scholars understood that the public has palpable and nuanced views on foreign policy, and that there is both a political and ethical responsibility to involve the public in matters of such import (Rottinghaus, 2008; Klarevas, 2002). Citizens have become more informed and vocal so that public support can encourage the onset of military operations, and are a vital indicator of its perceived success (Klarevas, 2002). In democratic countries, public attitudes create political incentives to make particular decisions, a fact that is no less true in the decision to use force. Multiple studies attest to the strategic influence of public attitudes on political decision-making regarding war due to fears of public backlash, political consequences, and the effect of public dissensus on morale (Meernik & Brown, 2007; Gelpi, 2006; Foyle, 2004; Klarevas, 2002; Sobel, 2001).

We offer four distinct reasons why public support plays a crucial role in the use of cyber force. First, public attitudes towards military operations are strongly correlated with the human costs of fighting—otherwise known as the principle of casualty aversion (Gelpi et al., 2006). A perceived attraction of cyber warfare is that combatants remain far from any physical battleground and there is a minimal threat to the lives of soldiers. This offers an advantage to political leaders who invariably come under considerable public pressure to ensure that military forces do not sustain mounting casualties (Schörnig, 2014; Osakweh & Umoh, 2013). While military casualties are a prime consideration in determining public support for the use of force, the public also takes into account civilian casualties on the enemy side (Ward, 2020; Schuurman, 2013; Johns & Davies, 2019; Walsh, 2015; Eichenberg, 2005). These studies, conducted in the United States and the United Kingdom, produce consistent evidence of civilian casualty aversion such that higher death tolls contribute to a decrease in support for force. Under these conditions, cyber weaponry is likely to capture the public imagination to the extent that it is viewed as a highly accurate and precise weapon, and notably, as a weapon that will minimize friendly and collateral civilian casualties (Hare, 2019).

Second, the public perceives cyber weaponry as sophisticated and advanced technology (Jarvis et al., 2014; Cavelty, 2012), in a way that encourages the glorification of its utility. Looking back, for example, at the early deployment of airpower during World War I, the United States witnessed a groundswell of public support for its use that had a definite impact on its deployment. During this period, society linked "technological advances in warfare to a rationalised teleology that [led] inexorably to aerial bombardment" (Kaplan, 2006, p. 400). The

American public was awestruck by the dramatic technological revolution that aerial power portended, and it recognized the utility of airpower as a low-risk military option, leading to heightened public support for its use (Vick, 2015). We can view a strong parallel between this historical situation and cyber power today. The public view of cyber power is that it is highly advanced, effective, and professional, which is likely to encourage public support for its deployment (Rubenstein, 2014).

Third, in addition to destroying or disrupting enemy assets, retaliatory cyber-attacks carry a public relations message as they respond to and affect public opinion. Military officials are increasingly publicizing what were once secretive cyber operations in order to signal resolve and capability (both domestically and externally), and to legitimize major investments in the cyber domain (Jacobsen & Ringmose, 2017; Egloff, 2020; Lindsay, 2015; Giles & Hartmann, 2019). We witnessed an example of this in the aftermath of a sophisticated cyber-attack by Iranian operatives against Israel’s water reservoirs in May 2020. In response to mounting domestic anger and calls for retaliation, Israel publicly conducted a damaging cyber-attack against Iranian ports, at least partly with the aim of expressing resolve to a domestic audience and demonstrating its cyber-prowess to deter adversaries (Bergman & Halbfinger, 2020).

Fourth, the public has a role to play in the development of norms regarding offensive weapons and cyberspace. The last decade has seen an intensifying public debate about cyberspace sovereignty, which many have characterized as a debate about the future of the Internet itself (Meyer, 2020; Hollis & Ohlin, 2018). To date, the Internet has operated according to a multi-stakeholder model that views cyberspace as a neutral domain that should remain free from overt militarization and restrictive national management. Yet there are mounting calls from countries that seek to “securitize” cyberspace by shifting norms of surveillance and privacy (Klimburg, 2020). Until now, countries have refrained from taking that final step towards embracing physically catastrophic cyber-attacks, and the public tolerance for norm-breaking behavior that will alter the nature of cyberspace is a factor to consider (Klimburg, 2020; Leuprecht et al., 2019). If the public view were entirely ignored, this could lead to a gap in perceptions about appropriate cyber policy between the public, military, and civilian elites, which can in turn undermine public support for democratic institutions and decisions to use force (see for example Shields, 2020).

Despite these arguments, the debate surrounding the effects of public opinion on cyber operations remains unsettled. In some instances, the secrecy of cyber operations minimizes the need for public mobilization before the fact (see Shane, 2020 for a review of the claim). Likewise, the attribution challenges that plague cyberspace, and the lack of public expertise in cyber affairs often derogates the public position to one of spectator. Nevertheless, there is a definitive trend wherein militaries are publicizing once secretive cyber strikes to legitimize major investments, to undermine the enemy’s trust in their IT infrastructure, and to signal cyber-strength to potential adversaries—all of which overturn the historical perception of cyber-attacks as entirely clandestine acts (Jacobsen & Ringsmose, 2017).

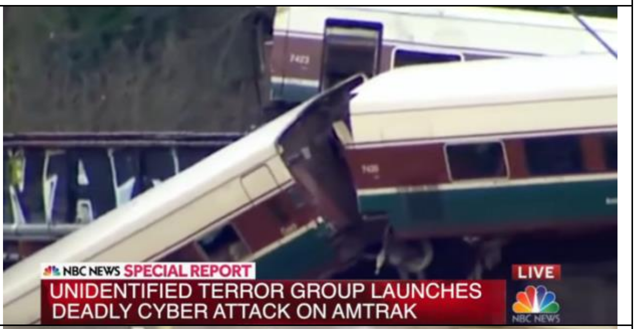
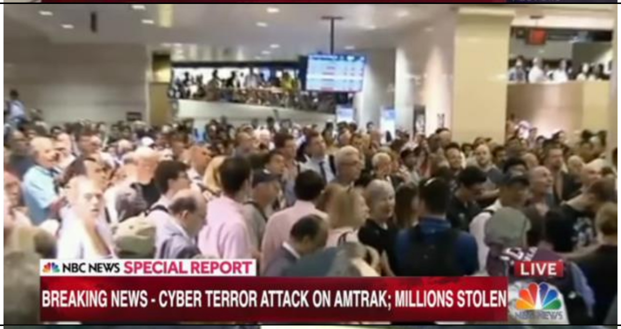
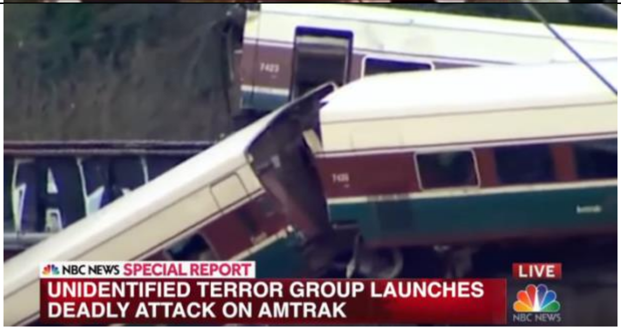
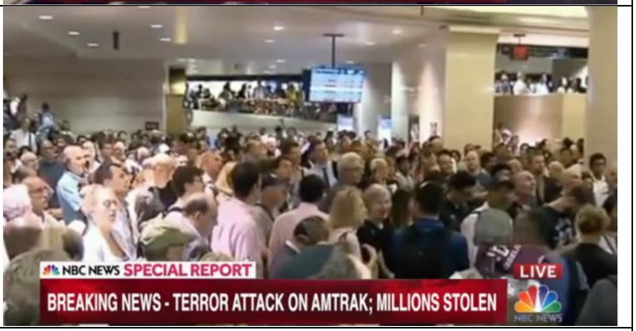
In view of these rationales, study 1 tests the hypothesis that *(H1) public support will be greater for retaliatory military strikes using cyber means rather than conventional (kinetic) means*. We further suggest that the public support for using cyber weapons in retaliatory strikes will be predicated on the view of cyber power being a strong military response, yet one that is still less destructive in that it will not cause lethal consequences or target civilians. As such, study 1 and 2 collectively test the hypothesis that *(H2) the preference for cyber retaliation will dissipate to the extent that respondents become aware of the capacity of cyber-attacks to cause destructive and lethal consequences*.

Experimental Methodology

To test these hypotheses, we conducted two controlled and randomized survey experiments that exposed respondents to simulated video news broadcasts reporting on various forms of terror attacks on their home soil. Experiments in recent years have shown how exposure to broadcast videos and media reports of terror attacks are sufficient to cause variations in emotional and political attitudes (Backhaus et al., 2020; Shandler et al., 2021; Canetti et al., 2017; Gross et al., 2017). We elected to utilize professionally produced television news reports since they offer a vivid experimental manipulation that is more authentic than vignettes or fabricated newspaper articles, which are the norm in many survey experiments about international security. We simultaneously ran this experiment in three countries (the United States, the United Kingdom, and Israel). We selected these settings since each of these countries are susceptible to terror attacks, and all have credibly been involved in retaliatory strikes following terror events, heightening the aura of credibility around the scenarios. This authenticity factor was also the reason why the scenarios focused on terror attacks and not inter-state attacks. Further to this, each of the selected countries is ranked within the same decile in terms of the social and economic impact of terrorism as measured by the Global Terrorism Index (Institute for Economics & Peace, 2017).

Respondents were randomly allocated to one of five experimental conditions reflecting a 2X2 experimental design with a control group. Each condition viewed an original, professionally produced television news report (M*time* = 1min 32sec) that purported to have broadcast on local news stations in the three countries—NBC News in the United States, Sky News in the United Kingdom, and Channel 2 in Israel. The news stories reported about a terror attack against railway infrastructure. (See online appendix A for complete scripts and video screenshots).[1] The manipulations differed regarding the method of the terror attack (cyber terror vs. conventional [kinetic] terror) and the consequences of the terror attack (causing fatalities vs. causing financial damage). Participants allocated to a control group did not view any news stories or receive any treatment to influence their responses to the questionnaire. The video news reports were identical in each country, with only minor adaptations in order to refer to local cities and railway companies, and with the relevant music and logos of each broadcaster. Table 1 describes the differences among the manipulation conditions.

Table I. Description of video manipulation conditions

Treatment Condition	Method of attack	Consequences of attack	Screenshot from Breaking News Report
Lethal cyber terror attack condition	Cyber-attack	The attack caused a train to derail, killing 7 passengers and injuring 10 passengers.	 NBC NEWS SPECIAL REPORT UNIDENTIFIED TERROR GROUP LAUNCHES DEADLY CYBER ATTACK ON AMTRAK LIVE NBC NEWS
Non-lethal cyber terror attack condition	Cyber-attack	The attack resulted in the theft of tens of millions of dollars from the railway company's passengers' credit cards.	 NBC NEWS SPECIAL REPORT BREAKING NEWS - CYBER TERROR ATTACK ON AMTRAK; MILLIONS STOLEN LIVE NBC NEWS
Lethal conventional terror attack condition	Conventional / kinetic attack	The attack caused a train to derail, killing 7 passengers and injuring 10 passengers.	 NBC NEWS SPECIAL REPORT UNIDENTIFIED TERROR GROUP LAUNCHES DEADLY ATTACK ON AMTRAK LIVE NBC NEWS
Non-lethal conventional terror attack condition	Conventional / kinetic attack	The attack resulted in the theft of tens of millions of dollars from the railway company's passengers' credit cards.	 NBC NEWS SPECIAL REPORT BREAKING NEWS - TERROR ATTACK ON AMTRAK; MILLIONS STOLEN LIVE NBC NEWS
Control condition	N/A	Did not view any video	Did not view any video

Note: Screenshots are taken from the U.S. video news reports

Study 1: Discerning Consistently Higher Public Support for Cyber Retaliatory Strikes

Respondents (n = 1,848, approximately 600 in each of the three countries) were randomly assigned to one of five experimental conditions (see table 1) over a three-day period from October 14 to October 17, 2018. The survey-experiment was disseminated via online survey companies (Amazon Mechanical Turk, Prolific, and Midgam) in the United States, United Kingdom, and Israel respectively. After viewing the video, respondents completed a detailed questionnaire. In line with institutional review board requirements, respondents were first screened for post-traumatic stress disorder. Recognizing the graphic and ultra-realistic nature of the experimental video treatments, respondents who reported post-traumatic stress symptoms or had recent experience with any form of trauma were excluded from the study.[2] An attention check was conducted following the manipulation leading to the exclusion of 16 respondents (0.8% of the total). The study respondents represented a cross study of the general population in each country (United States: N=597, Mage= 37 years, SD =10.37; United Kingdom: N=597, Mage= 37 years, SD = 11.93; and Israel: N=638, Mage = 39, SD = 13.19). The political orientation of the sample in Israel skewed further to the right compared to the American and British sample, and the British sample had a greater proportion of female respondents than in the United States and Israel. Online appendix B presents detailed statistics of the sample and balance checks across the conditions.

Measures

The independent variable is exposure to terrorism. This variable is based upon the simulated video news reports described above. The five conditions are: 1) lethal cyber-terrorism; 2) non-lethal cyber-terrorism; 3) lethal conventional terrorism; 4) non-lethal conventional terrorism; 5) control condition.

The two primary dependent variables that were measured are 1) support for retaliatory cyber strikes; and 2) support for retaliatory missile strikes. These were measured using a six-item summative index of retaliatory responses previously used in experimental research by Gross et al. (2017) and Graves et al. (2014). For each of the two sets of retaliatory options, respondents were asked to indicate their support for the various military responses in the aftermath of attacks on the soil of their respective countries. Retaliatory options included cyber or missile attacks aiming at military or civilian targets. (For example, to what extent do you support missile strikes against military targets of the attacker; to what extent do you support a cyber-attack against civilian targets (banks, railways, airports) and military targets of an attacker?) All items were rated on a scale of 1 (not at all) to 6 (absolutely). Two items pertaining to non-violent response options (economic sanctions and diplomatic protest) were removed, leaving four items in total. Post-hoc analysis showed the scales to be only moderately reliable due to variance in support for targeting civilian or military infrastructure (Cronbach's α = .64 for cyber retaliation; Cronbach's α = .69 for kinetic retaliation).[3]

The covariates that were collected included age, gender, level of education, self-identified political orientation, family income, computer literacy (a summative index of four items taken from Hargittai & Hsieh, 2012), frequency of public transportation usage, and anxiety following exposure to the video manipulations (measured using the Short Form Spielberger State-Anxiety Inventory developed by Spielberger, 1970).

Results

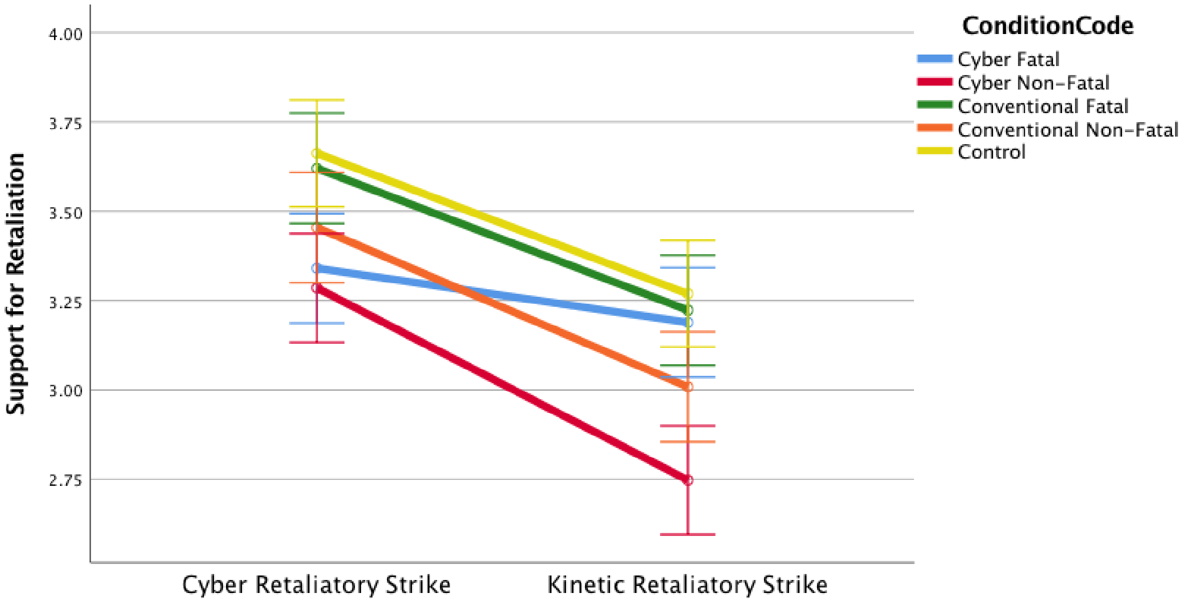
The first step of our analysis strategy was to explore any variance in support for cyber and kinetic retaliatory strikes following exposure to our distinctive terror conditions. Table 2 summarizes the mean scores for each of the two dependent variables (support for cyber retaliatory strikes, and support for retaliatory strikes using missiles) showing the level of support by country and terror condition, while figure 1 illustrates the paired group comparisons.

Table II. Means for respondents on retaliation measures

Country	**Treatment condition**	**N**	**Support for cyber retaliatory strikes**	**Support for kinetic retaliatory strikes**
United States	Cyber Terror - Fatal	118	3.28	3.19
	Cyber Terror – Non-Fatal	119	3.20	2.69
	Conventional Terror - Fatal	119	3.34	3.07
	Conventional Terror – Non-Fatal	116	3.23	2.91
	Control	125	3.65	3.24
United Kingdom	Cyber Terror - Fatal	120	2.63	2.46
	Cyber Terror – Non-Fatal	119	2.70	2.11
	Conventional Terror - Fatal	118	3.04	2.57
	Conventional Terror – Non-Fatal	120	2.77	2.28
	Control	120	2.85	2.37
Israel	Cyber Terror - Fatal	125	4.07	3.89
	Cyber Terror – Non-Fatal	130	3.90	3.38
	Conventional Terror - Fatal	122	4.45	4.00
	Conventional Terror – Non-Fatal	123	4.33	3.81
	Control	138	4.38	4.08
Combined countries	Cyber Terror - Fatal	363	3.34	3.19
	Cyber Terror – Non-Fatal	368	3.29	2.75
	Conventional Terror - Fatal	359	3.62	3.22
	Conventional Terror – Non-Fatal	359	3.45	3.01
	Control	383	3.66	3.27

All measures are scored on a scale from 1 – 6 where 1 represents the lowest and 6 represents the highest score.

Figure 1. Comparing support for cyber and kinetic retaliatory strikes by terror condition among all countries

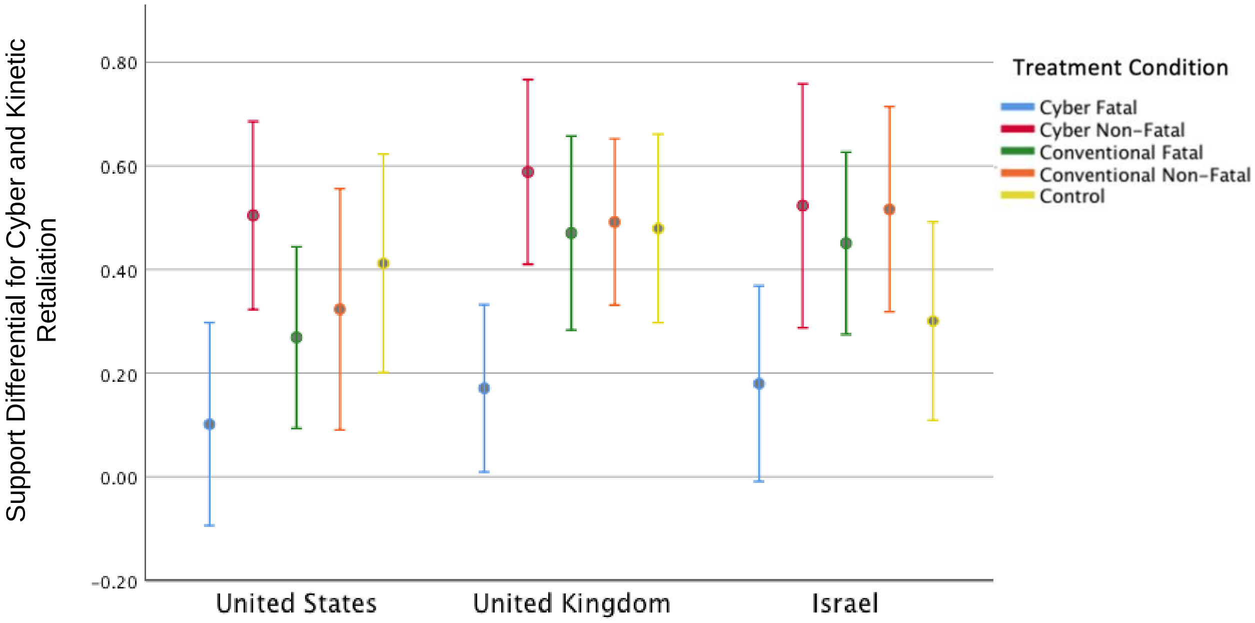


Error bars reflect 95% confidence intervals.
All measures are scored on a scale from 1 – 6 where 1 represents the lowest and 6 represents the highest score.

Observing the between-group effects, we see that support for retaliatory strikes generally (both cyber and kinetic) is uniformly higher when respondents are exposed to terror attacks causing lethal consequences. This is consistent with previous research suggesting that retaliatory intent rises with the number of in-group members killed (Kreps & Das, 2017). This effect holds when looking at a combined dataset and also on the individual country level. Though the overall level of support for retaliation increases and decreases between the three countries in line with their particular national attitudes toward military power and retaliation (Stein, 2015), the pattern of increased support for retaliation following fatal terror strikes remains constant. We note an unanticipated finding that the respondents in the control condition, who did not view any experimental manipulation, exhibited among the highest levels of support for retaliation. This can be explained by the fact that the control group indicated their level of support for military retaliation without information about the type or severity of the incident. In these circumstances, the control respondents in each country naturally and uniformly assumed a worst-case scenario (i.e. a high casualty terror attack). We ran a post-hoc experiment with a new dataset (N=737) that confirmed this explanation (see online appendix C for the full post-hoc analysis). While interesting in itself, this does not preclude the effective use of the control condition as a neutral reference group in the subsequent analyses.

More importantly, what is clear from the descriptive data is that among all conditions, support for cyber retaliatory strikes is higher than for retaliatory strikes using missiles. This offers initial credence to our first hypothesis that predicted higher support for cyber retaliation. Yet as can be seen in figure 1, the descending slope of within-group comparisons is discernibly flatter for one experimental condition—exposure to lethal cyber terror. According to our second hypothesis, we expect that heightened knowledge about the potentially lethal characteristics of cyber-attacks will contribute to decreased relative support for cyber over kinetic strikes. The lethal cyber-terror condition, in which respondents were exposed to news reports about cyber strikes causing fatal consequences, constitutes the requisite knowledge to meet this familiarity threshold. Figure 2 demonstrates the extent of these slopes by representing the differential support for cyber over kinetic military strikes within the underlying country level data (error bars reflect 95% confidence intervals). Consistently among all three countries, the differential support in the cyber-fatal condition is significantly lower than all other conditions.

Figure 2. Differences between levels of support for cyber and kinetic retaliation by terror condition and country



Note: The measured variance reflects the level of support for cyber retaliatory strikes minus support for kinetic retaliatory strikes. A larger positive integer on the y-axis therefore reflects greater support for cyber strikes relative to kinetic strikes, while a negative integer on the y-axis reflects greater support for kinetic strikes relative to cyber strikes.
Error bars reflect 95% confidence intervals. Circles reflect the item mean.

To test the significance of these findings, we ran a series of four ordinary least squares regression analyses—one for each of the three countries and another with a combined multi-country dataset (see table 3). In the past we would have run these analyses with the difference scores as the dependent variable (i.e. support for cyber retaliation minus support for kinetic retaliation). Yet the literature has slowly developed a preference for comparing differences across groups by including one variable as the dependent variable and controlling for the other as one of the predictor variables (Jennings & Cribbie, 2016; Edwards, 2002; Edwards, 1995). In line with this approach, the dependent variable in our analysis is support for cyber retaliation, while support for kinetic retaliation appears as a covariate. Each of the experimental terror conditions was inserted as a dummy variable with the fatal cyber-terror group acting as the reference condition. In addition to these variables, we entered various covariates that have historically been associated with militant attitudes such as age, gender, political orientation, anger, anxiety, and previous exposure to terror incidents. The results reveal a significantly higher level of support for using cyber weapons among all conditions relative to the cyber-lethal condition. This effect holds while controlling for other covariates including support for using kinetic weapons. The findings also reveal that both gender and political orientation contribute to this differential support. To the extent that respondents are male or more right-wing, the difference in support for cyber and kinetic retaliatory strikes will be lower. Put another way, these characteristics will decrease the likelihood of supporting cyber strikes to a greater extent than kinetic strikes. This corresponds with past research that confirmed a consistent gender gap in support for military conflict in multi-country settings (Wilcox et al., 1996; Togeby, 1994).

Table III. OLS regression models of differential support for cyber and kinetic retaliatory strikes

	(1) -------- Combined Country Sample	(2) -------- U.S.	(3) -------- U.K.	(4) -------- Israel
Cyber terror (non-fatal) Condition – dummy variable	.247*** [.001]	.266* [.043]	.336** [.006]	.152 [.236]
Conventional terror (fatal) Condition – dummy variable	.251*** [.001]	.120 [.354]	.322** [.008]	.312* [.016]
Conventional terror (non-fatal) Condition – dummy variable	.242*** [.001]	.280 [.125]	.303* [.012]	.286* [.029]
Cyber terror (non-fatal) Condition – dummy variable	.283*** [.000]	.389** [.004]	.327** [.009]	.181 [.159]
Political orientation (1 = very left wing, 7 = very right wing)	.009 [.598]	.088 [.726]	-.003 [.911]	-.031** [.336]
Age	.000 [.630]	-.002 [.533]	-.002 [.580]	.000 [.646]
Gender (0 = male; 1 = female)	-.283*** [.000]	-.279*** [.001]	-.250** [.002]	-.308*** [.000]
Previous exposure to terror attacks (0 = no exposure, 1 = exposure)	.066 [.152]	-.054 [.518]	.074 [.337]	.166* [.041]
Anger	.039 [.109]	.041 [.297]	.068 [.118]	-.009 [.844]
Anxiety	-.014 [.590]	.013 [.776]	-.042 [.391]	.008 [.865]
Support for kinetic retaliation	.674*** [.000]	.652*** [.000]	.769*** [.000]	.612*** [.000]
Country dummies	Yes	No	No	No
Observations	1,832	597	597	638
R-squared	.575	.519	.539	.455
Adjusted R-squared	.572	.510	.530	.445

The dependent variable in these analyses is support cyber retaliation while controlling for support for kinetic retaliation. Regression coefficients with p-values in brackets.
Country dummies covariate indicates whether dummy variables for each country were included in the model's analysis.
$* p < 0.05$; $** p < 0.01$; $*** p < 0.001$

To more closely examine the differences between support for cyber and kinetic retaliation between each of the experimental conditions, we ran a series of paired t-tests (see table 4). This allows us to observe the significance of the difference in support between each of the individual treatment groups. Paired group comparisons were conducted with a Bonferroni correction to control for the number of comparisons in each country sample, yielding an alpha level of .01 (.05/5). The data reveals that even with the harsh Bonferroni adjustment, there was still significantly higher support for cyber weapons in each of the three countries for those respondents in conditions 2 – 5. Yet as expected, the difference in support for cyber and kinetic retaliation was not significant for the fatal cyber-terror condition.

Table IV. Paired t-test analyses comparing support for cyber and kinetic strikes by terror conditions and country

			United States				**United Kingdom**				**Israel**			
	Terror condition		N	Mean	Diff	t (df)	N	Mean	Diff	t (df)	N	Mean	Diff	t (df)
1	Cyber terror - fatal	Cyber retaliation	118	3.29	.10	1.03 ***n.s.*** (117)	120	2.63	.17	2.10 ***n.s.*** (119)	125	4.07	.18	1.89 ***n.s.*** (124)
		Kinetic retaliation	118	3.19			120	2.46			125	3.89		
2	Cyber terror – non-fatal	Cyber retaliation	119	3.20	.50	5.51 * (118)	119	2.70	.591	6.53 * (118)	130	3.90	.52	4.40 * (129)
		Kinetic retaliation	119	2.69			119	2.11			130	3.38		
3	Conventional terror - fatal	Cyber retaliation	119	3.34	.27	3.04 * (118)	118	3.04	.47	4.98 * (117)	122	4.45	.45	5.07 * (121)
		Kinetic retaliation	119	3.07			118	2.57			122	4.00		
4	Conventional terror – non-fatal	Cyber retaliation	116	3.23	.32	2.76 * (115)	120	2.77	.49	6.08 * (119)	123	4.33	.52	5.16 * (122)
		Kinetic retaliation	116	2.91			120	2.28			123	3.81		
5	Control	Cyber retaliation	125	3.65	.41	3.87 * (124)	120	2.85	.48	5.21 * (119)	138	4.38	.30	3.11 * (137)
		Kinetic retaliation	125	3.24			120	2.37			138	4.08		

** Significant with Bonferroni correction (p < 0.01).*

Study 2: Exposure to lethal cyber-attacks undermines the illusion of cyber as a non-violent domain and neutralizes the preference for cyber strikes

While study 1 demonstrated that those exposed to lethal cyber terror strikes exhibit lower support for retaliating with cyber weapons, the findings do not offer sufficient empirical evidence about why this is the case. Study 2 therefore seeks to build on the first study to examine the rationale for this support differential. We hypothesized that people who are exposed to lethal cyber-attacks develop a newfound understanding that cyber weapons can cause physically destructive and even fatal consequences, which explains their relative caution in using these weapons. To test this theory, we conducted a second online survey experiment with a new sample of respondents in the United States, the United Kingdom, and Israel. Once again, we randomly allocated respondents (n = 737) into the same five experimental conditions. Each condition viewed the same professionally produced video news report that purported to have broadcast on local news stations in the three countries. The survey was disseminated on February 27, 2020,[4] using online survey companies (Amazon Mechanical Turk, Prolific, and Midgam) in the United States, United Kingdom, and Israel. An attention check was conducted following the manipulation leading to the exclusion of 3 respondents (0.4% of the total). The study respondents represented a cross section of the general population in each country (United States: N=246, Mage= 38 years, SD =11.22; United Kingdom: N=235, Mage= 36 years, SD = 10.86; and Israel: N=253, Mage = 41, SD = 13.67).

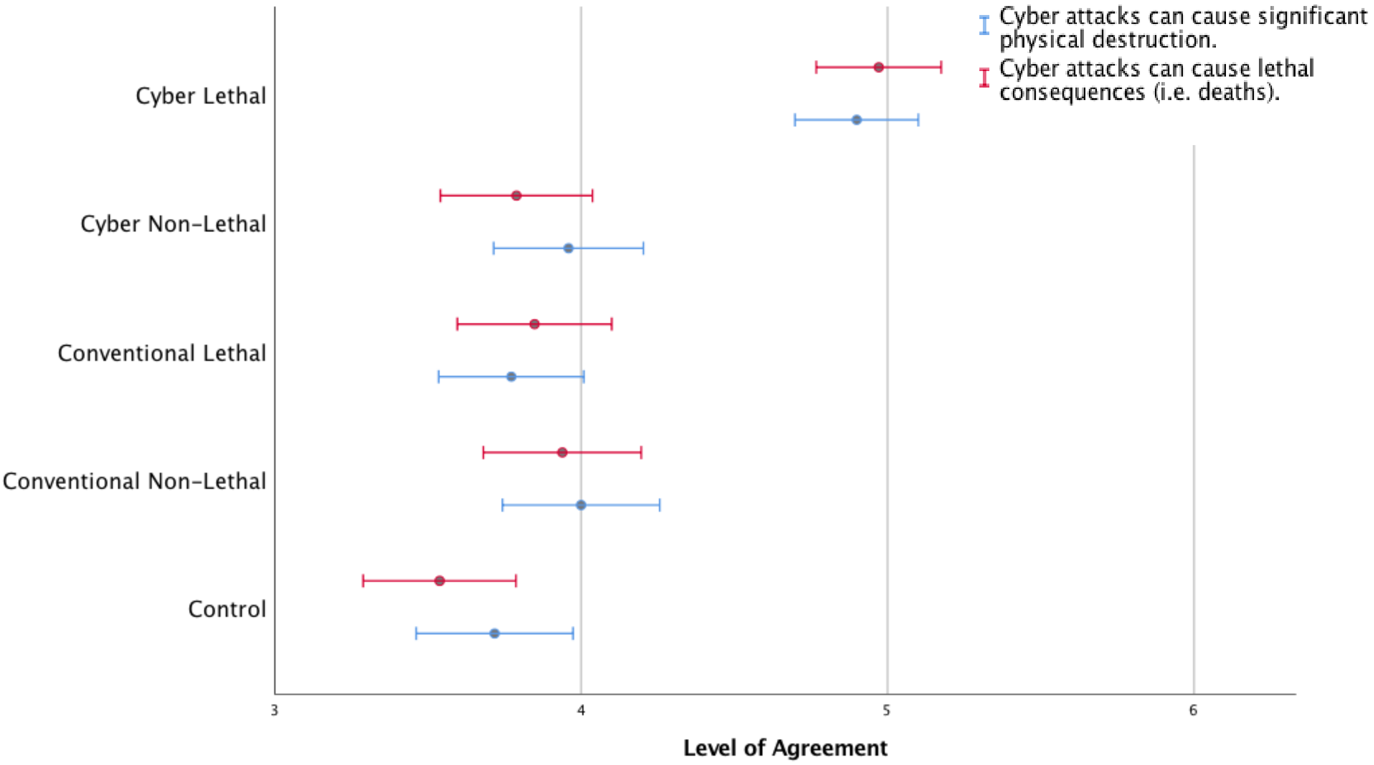
In addition to the measures that appeared in study 1, we added an additional measure in an attempt to scrutinize the reasons behind the support (or lack thereof) for deploying cyber force. Respondents indicated their level of agreement with two statements relating to the nature of cyber weapons. (1) "Cyber-attacks can cause significant physical destruction"; and (2) "Cyber-attacks can cause lethal consequences (i.e. deaths)." All items were rated on a scale of 1 (not at all) to 6 (absolutely).

Results

As a first step, we replicated and corroborated the results of study 1 with the new sample. Once again, we observed a statistically significantly higher level of support for using cyber weapons compared to conventional weapons for all respondents—apart from those in the group that was exposed to the cyber-lethal manipulation. This outcome was consistent among all countries. The paired T-test analyses for the new sample appear in online appendix D.

According to our theory that exposure to a cyber-lethal attack increases understanding of the destructive and lethal capacity of cyber weapons, we would expect to see a significantly higher level of agreement from participants in the cyber-lethal condition with statement 1 (cyber-attacks can cause significant physical destruction) and statement 2 (cyber-attacks can cause lethal consequences (i.e. deaths)). As illustrated in figure 3, the levels of support for the two statements are visibly and significantly higher for the cyber-lethal condition compared to all four other conditions. The mean level of support in the cyber-lethal condition for the assertion that cyber-attacks can cause significant physical destruction is 4.90, while the mean support among the other four conditions ranges from 3.54 to 3.96. For the assertion that cyber-attacks can cause lethal consequences, the mean level of support for the cyber-lethal condition registers at 4.97, while the mean support in the other four conditions ranges from 3.54 to 3.94.

Figure 3. Level of agreement with statements on the nature of cyber attacks



Error bars reflect 95% confidence intervals. Circles reflect the item mean.

We then ran a set of two ordinary least squares regression analyses for each of the two statements (see table 5). Each of the experimental terror conditions was inserted as dummy variables with the fatal cyber-terror group acting as the reference condition. Likewise, each of the countries was inserted as dummy variables with Israel acting as the reference condition. In addition, we entered various covariates that may influence understanding of cyber issues (age, gender, political orientation, anxiety levels following exposure to the manipulation, and computer literacy).

The results clearly demonstrate that respondents who were exposed to lethal cyber-attacks view cyber weapons as bearing physically destructive and lethal qualities at significantly higher rates than all other respondents (p < .000 among all four conditions). This effect persists when controlling for differences between the three countries, though Israeli respondents seem to view cyber weapons as more physically destructive and lethal than American and British respondents. The effect also remains consistent when controlling for the covariates. Gender and computer literacy are significant contributing factors in both models, with men more likely to agree with the statements on the nature of cyber weapons, while computer literacy is significantly positively associated with viewing cyber weapons as destructive and lethal (for more on the effect of domain knowledge, see Gomez & Villar, 2018). In online appendix E we run a robustness test that demonstrates that attitudes toward cyber weapons among respondents exposed to lethal cyber-attacks do not fundamentally shift in all aspects, only in regards to perceptions of destructiveness and lethality.

Table V. OLS regression models of support for statements about nature of cyber weapons

	Statement 1 **--------** **‘Cyber attacks can cause significant physical destruction’**		**Statement 2** **--------** **‘Cyber attacks can cause lethal consequences’**	
Cyber terror (non-fatal) Condition – dummy variable	-.955*** [.000]	-.950*** [.000]	-1.191*** [.000]	-1.164*** [.000]
Conventional terror (fatal) Condition – dummy variable	-1.143*** [.000]	-1.156*** [.000]	-1.134*** [.000]	-1.137*** [.000]
Conventional terror (non-fatal) Condition – dummy variable	-.914*** [.000]	-.849*** [.000]	-1.041*** [.000]	-.945 *** [.000]
Control condition – dummy variable	-1.199*** [.000]	-1.175*** [.000]	-1.444*** [.000]	-1.373*** [.000]
Country – United States – dummy variable	-.620*** [.000]	-.753 *** [.000]	-.390** [.003]	-.466*** [.001]
Country – United Kingdom – dummy variable	-.558 *** [.000]	-.518 *** [.000]	-.398** [.003]	-.219 [.144]
Age		.000 [.943]		.003 [.467]
Gender (0 = male; 1 = female)		-.249* [.034]		-.467*** [.000]
Level of anxiety following experimental treatment		.036 [.438]		.086 [.070]
Political orientation (1 = left wing, 7 = right wing)		-.014 [.698]		.023 [.525]
Computer literacy		.123** [.008]		.112* [.016]
Observations	734	734	734	734
R-squared	.109	.130	.111	.149
Adjusted R-squared	.102	.117	.104	.137

Regression coefficients with p-values in brackets.
$* p < 0.05$; $** p < 0.01$; $*** p < 0.001$

Discussion and Conclusion

Under what circumstances does the public support the use of cyber strikes? There is a long-running debate between scholars who explain that cyber warfare will lead to uninhibited escalation, and those who advocate for why cyber tools will encourage restraint and lower the propensity of conflict. This article proposes that both sides have ignored the crucial role of public support for conducting cyber strikes. While public opinion is not a decisive factor in matters of foreign affairs, it has a key role to play in cyber warfare since many of the benefits of cyber weapons relate to the ability of cyber strikes to relieve public pressure on political leaders by reducing the human costs of war. As such, we present the results of two interconnected survey experiments that measure public support for cyber versus conventional military retaliation in three countries - the United States, United Kingdom, and Israel.

The two studies identify strong public support for the use of cyber weapons as part of retaliatory strikes following cyber and conventional terror attacks. This makes sense, since cyber strikes offer a compelling lure to a public that is wary of friendly and civilian casualties (Gelpi et al., 2006). Yet we demonstrate that *public support for cyber strikes is fragile*. It is predicated on a perception of cyber operations as a safe, non-threatening, and non-destructive alternative to conventional military weapons. Once the public is exposed to lethal or physically destructive cyber-attacks, the illusion of cyber as a non-destructive domain is undermined and the public preference for cyber weapons disappears.

Applying these findings to military decision-making, we assert that the current public preference for the use of cyber tools could contribute to a cyber-mediated military escalation since governments that have refrained from using military force due to fear of civilian sentiment can now overcome that obstacle. While scholars and military theorists have offered persuasive claims about the de-escalating potential of cyber weapons, they have failed to account for the variable of robust public preference for the use of cyber tools.

The fact that this cyber-preference was consistently identified in six datasets across three countries speaks to its robustness. Interestingly, respondents in the three countries demonstrated significantly different levels of preference for retaliation. On a six-point scale, where one indicates the lowest support, and six indicates absolute support, Israeli respondents registered an average of 4.02 in their support for retaliation, while the more conciliatory British respondents indicated support for retaliation at only 2.58 scale points. American responses fell in between these two extremes. Yet despite this vast difference in overall support for retaliation, each of the three countries exhibited an identical preference for using cyber weapons over their conventional counterparts. And in each of the three countries, this preference dissipated only amongst those respondents who were exposed to information about the destructive and lethal capacity of cyber strikes.

Importantly, this preference for the use of cyber tools is even apparent following conventional attacks. This is noteworthy, since it plays into an ongoing discussion about cross-domain escalation, that is, whether the public is willing to escalate with kinetic force (air strikes, etc.) in response to attacks that took place purely within the cyber domain. While Gross et al. (2016; 2017) offered initial evidence that the public is willing to retaliate against cyber-attacks with conventional physical weapons, Kreps and Schneider (2019) found that individuals are highly reluctant to escalate with kinetic force in response to attacks that take place purely in the cyber domain. By imputing the presence of a firebreak that prevents cross-domain escalation, Kreps and Schneider (2019) theorized that members of the public perceive cyber operations as something distinct from conventional military operations. Our study adds a new level to these findings by demonstrating that the public preference for cyber retaliation—within-domain or cross-domain—is contingent on their being viewed as less destructive. Once this perception is undermined by exposure to destructive cyber-attacks, the public preference for using cyber weapons disappears, since cyber weapons are no longer viewed as categorically different than their conventional counterparts.

Our new understanding of the reasons behind the support for using cyber weapons suggests that it will run into an impending ceiling. Cyber weapons, be it in the hands of terror groups or state entities, are beginning to develop the potential to exert destructive and lethal consequences. We offer several recent examples to support this claim. A recent cyber-attack by Iranian-linked operatives successfully breached the control systems of Israel’s civilian water infrastructure (Heller, 2020). Several months later, a cyber-attack against a hospital in

Düsseldorf resulted in a patient's death after the attack caused emergency surgery to be postponed (Tidy, 2020). Furthermore, a 2018 report published by the United States Department of Homeland Security explained that Russian cyber operatives had infiltrated control rooms of U.S. power plants and possessed the ability to remotely control critical components of the electricity grid (Sanger, 2018). Our findings suggest that as these destructive and lethal characteristics continue to come to light, public support for employing cyber tools will fall relative to support for non-cyber weapons.

We envision that the public will offer strong support for using cyber-attacks against terror operatives, but only until they are exposed to its lethal effects. This knowledge will not be hard to come by since the consequences of military or terror attacks are commonly publicized, even though attribution in the cyber realm can be challenging. But this also raises a dilemma for political and military policymakers. According to our findings, the military would only have one opportunity to conduct a (publicly revealed) cyber-attack with physically destructive consequences before the window of heightened public support wanes. This mirrors a frequent critique that the deployment of cyber weapons reduces their future effectiveness, since rivals can remedy the digital weaknesses that the attacks exploit.

To maximize the authenticity of the experimental manipulations, this research focused on attitudes in the aftermath of terror incidents. We encourage future research to extend these findings to attitudes following state-level attacks, and also proactive military operations (i.e. not retaliation). We also encourage comparative studies that consider how this theory applies to other developing unorthodox military capabilities such as drones and orbital weapons.

In line with our commitment to avoid falling prey to the hyperbolic warnings that have characterized past military technological revolutions, we note that public support for cyber weapons is only significant in predicting its use to the extent that the public plays a role in foreign policy decision making. Where governments are more susceptible to public pressure regarding the use of force, the effect of public support will be stronger. Governments and non-government actors alike have exercised caution up until this point in executing cyber strikes, with most attacks limited to minor defacements or denial of service attacks, despite the existence of more damaging capabilities (Valeriano & Maness, 2014). While public support can encourage the use of force, it can also set boundaries on the measures that governments can legitimately use. Indeed, as public support for the use of cyber tools wanes in the aftermath of destructive attacks, a possible consequence is that the public could constrain governments that are otherwise enthusiastic about employing cyber strikes. In both scenarios, public support plays a key role, and it must be taken into account in future models of cyber warfare.

Endnotes

1 - The online appendix can be accessed at: https://doi.org/10.7910/DVN/7C1MGB

2 - In the aftermath of traditional and cyber terror attacks, research has shown how anger is a common emotional response (Lerner et al., 2003; Small et al., Fischhoff 2006). Likewise, terrorism aggravates feelings of anxiety (Canetti et al., 2016; Gross et al. 2017; Huddy et al., 2005). Respondents received a de-briefing following the survey that explained that the video news story was fabricated for the purposes of an academic study.

3 - Research has conclusively demonstrated that people's tolerance for risky military action shifts depending on several additional variables such as the identity of the adversary, and how the potential outcomes of military conflict are framed (Berejikian & Zwald, 2020). We hold these variables constant in each of our experimental treatment groups by offering no information about the details of the attack. As such, we focus on and isolate the retaliation type variable alone.

4 - The data collection took place before any COVID-19 related lockdowns or social distancing guidelines had been introduced in these three countries.

References

Acton, J. (2017). Cyber weapons and precision-guided munitions. In G. Perkovichand & A.E. Levite (Eds.), *Understanding Cyber Conflict: Fourteen Analogies* (pp. 45-60). Georgetown University Press.

Backhaus, S., Gross, M. L., Waismel-Manor, I., Cohen, H., & Canetti, D. (2020). A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking*, *23*(9), 595-603. https://doi.org/10.1089/cyber.2019.0692

Baum, M. A., & Potter, P. B. (2015). *War and democratic constraint: How the public influences foreign policy*. Princeton University Press.

Bergman, R., & Halbfinger, D. M. (2020, May 19) Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks. *The New York Times*. https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html

Berejikian, J., & Zwald, Z. (2020). Why language matters: Shaping public risk tolerance during deterrence crises. *Contemporary Security Policy*, 41(4), 507-540. https://doi.org/10.1080/13523260.2020.1729496

Brantly, A., & Smeets, M. (2020). Military Operations in Cyberspace. In *A. Sookermany (ed.), Handbook of Military Sciences* (pp. 1-16). https://doi.org/10.1007/978-3-030-02866-4_19-1

Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., & Cohen, H. (2017). How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychology, Behavior, and Social Networking*, *20*(2), 72-77. https://doi.org/10.1089/cyber.2016.0338

Canetti, D., Gross, M. L., & Waismel-Manor, I. (2016). In F. Allhoff, A. Henschke & B.J. Strawser (Eds.), *Binary Bullets: The Ethics of Cyberwarfare* (pp. 157-176*)*. Oxford University Press.

Cavelty, M. D. (2012, June). The militarisation of cyberspace: Why less may be better. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (pp. 1-13). IEEE.

Cavelty, M. D. (2010). *The reality and future of cyberwar* (Parliamentary brief). Zurich, Switzerland: CSS Analysis in Security Policy.

Denning, D. E. (2009). Barriers to entry: are they lower for cyber warfare?. *IO Journal*, *1*(1), 4-10. http://hdl.handle.net/10945/37162

Edwards, J. R. (2002). Alternatives to difference scores: Polynomial regression analysis and response surface methodology. In F. Drasgow & N. Schmitt (Eds.), *The Jossey-Bass business & management series. Measuring and analyzing behavior in organizations: Advances in measurement and data analysis* (pp. 350–400). Jossey-Bass.

Edwards, J. R. (1995). Alternatives to difference scores as dependent variables in the study of congruence in organizational research. *Organizational behavior and human decision processes*, *64*, 307-324. https://doi.org/10.1006/obhd.1995.1108

Egloff, F. J. (2020). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, *41*(1), 55-81. https://doi.org/10.1080/13523260.2019.1677324

Eichenberg, R. C. (2005). Victory has many friends: US public opinion and the use of military force, 1981–2005. *International security*, *30*(1), 140-177. https://doi.org/10.1162/0162288054894616

Eun, Y. S., & Aßmann, J. S. (2016). Cyberwar: Taking stock of security and warfare in the digital age. *International Studies Perspectives*, *17*(3), 343-360. https://doi.org/10.1111/insp.12073

Everts, P. (2000). When the going gets rough: does the public support the use of military force?. *World Affairs, 162*(3), 91-107. http://www.jstor.org/stable/20672578

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

Foyle, D. 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), 269-294. https://doi.org/10.1093/ijpor/edh025

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316-348. https://doi.org/10.1080/09636412.2015.1038188

Gelpi, C., Feaver, P. D., & Reifler, J. (2006). Success matters: Casualty sensitivity and the war in Iraq. *International Security*, *30*(3), 7-46. https://doi.org/10.1162/isec.2005.30.3.7

Giles, K., & Hartmann, K. (2019, May). Silent Battle Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-13). IEEE. https://doi.org/10.23919/CYCON.2019.8756713.

Gomez, M. A., & Villar, E. B. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*, *6*(2), 61-72. http://dx.doi.org/10.17645/pag.v6i2.1279

Gompert, D. C., & Libicki, M. (2014). Cyber warfare and Sino-American crisis instability. *Survival*, *56*(4), 7-22. https://doi.org/10.1080/00396338.2014.941543

Graves, J., Acquisti, A., & Anderson, R. (2014, May). Experimental measurement of attitudes regarding cybercrime. In *13th Annual Workshop on the Economics of Information Security. Pennsylvania State University*.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, *3*(1), 49-58. https://doi.org/10.1093/cybsec/tyw018

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284-291. https://doi.org/10.1080/00963402.2016.1216502

Hare, F. B. (2019). Precision cyber weapon systems: An important component of a responsible national security strategy?. *Contemporary Security Policy*, *40*(2), 193-213. https://doi.org/10.1080/13523260.2018.1529369

Hargittai, E., & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science Computer Review*, *30*(1), 95-107. https://doi.org/10.1177/0894439310397146

Heller, A. (2020, May 28). Israeli cyber chief: Major attack on water systems thwarted. *The Washington Post*. https://www.washingtonpost.com/world/middle_east/israeli-cyber-chief-major-attack-on-water-systems-thwarted/2020/05/28/5a923fa0-a0b5-11ea-be06-af5514ee0385_story.html

Hollis, D. B., & Ohlin, J. D. (2018). What if Cyberspace Were for Fighting?. *Ethics & International Affairs*, *32*(4), 441-456. https://doi.org/10.1017/S089267941800059X

Huddy, L., Feldman, S., Taber, C., & Lahav, G. (2005). Threat, anxiety, and support of antiterrorism policies. *American Journal of Political Science*, *49*(3), 593-608. https://doi.org/10.1111/j.1540-5907.2005.00144.x

Huntley, W. L. (2016, January). Strategic implications of offense and defense in cyberwar. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5588-5595). IEEE. https://doi.org/10.1109/HICSS.2016.691

Institute for Economics & Peace (2017). Measuring and understanding the impact of terrorism. *Institute for Economics and Peace*. http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf

Jacobsen, J. T., & Ringsmose, J. (2017). Cyber-bombing ISIS: why disclose what is better kept secret?. Global Affairs, 3(2), 125-137. https://doi.org/10.1080/23340460.2017.1337471

Jarvis, L., Nouri, L., & Whiting, A. (2014). Understanding, locating and constructing cyberterrorism. In Chen T., Jarvis L., Macdonald S. (Eds.), *Cyberterrorism* (pp. 25-41). Springer, New York, NY. https://doi.org/10.1007/978-1-4939-0962-9_2

Jennings, M., & Cribbie, R. A. (2016). Comparing pre-post change across groups: Guidelines for choosing between difference scores, ANCOVA, and residual change scores. *York Space Institutional Repository*. http://hdl.handle.net/10315/33240

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics: A Quarterly Journal of International Relations*, 30(2), 167-214. https://doi.org/10.2307/2009958

Johns, R., & Davies, G. A. (2019). Civilian casualties and public support for military action: Experimental evidence. *Journal of Conflict Resolution*, *63*(1), 251-281. https://doi.org/10.1177/0022002717729733

Kaplan, C. (2006). Mobility and war: the cosmic view of US ‘air power’. *Environment and Planning A*, *38*(2), 395-407. https://doi.org/10.1068/a37281

Klarevas, L. (2002). The “essential domino” of military operations: American public opinion and the use of force. *International Studies Perspectives*, *3*(4), 417-437. https://doi.org/10.1111/1528-3577.t01-1-00107

Klimburg, A. (2020). Mixed Signals: A Flawed Approach to Cyber Deterrence. *Survival*, *62*(1), 107-130. https://doi.org/10.1080/00396338.2020.1715071

Kostyuk, N., & Wayne, C. (2020). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogz077

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events?. *Journal of Conflict Resolution*, *63*(2), 317-347. https://doi.org/10.1177/0022002717737138

Krepinevich, A. F. (2012). *Cyber Warfare*. Center for Strategic and Budgetary Assessments. https://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf

Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*, *5*(1), 1-11. https://doi.org/10.1093/cybsec/tyz007

Kreps, S., & Das, D. (2017). Warring from the virtual to the real: Assessing the public’s threshold for war over cyber security. *Research & Politics*, *4*(2), 1-8. https://doi.org/10.1177/2053168017715930

Lerner, J. S., Gonzalez, R. M., Small, D. A., & Fischhoff, B. (2003). Effects of fear and anger on perceived risks of terrorism: A national field experiment. *Psychological science*, *14*(2), 144-150. https://doi.org/10.1111/1467-9280.01433

Leuprecht, C., Szeman, J., & Skillicorn, D. B. (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary Security Policy*, *40*(3), 382-407. https://doi.org/10.1080/13523260.2019.1590960

Lieber, K. (2014). The offense-defense balance and cyber warfare. In E.O. Goldman & J. Arquilla (Eds.), *Cyber Analogies* (pp. 96-107). Naval Postgraduate School, Monterey, California.

Liff, A. P. (2012). Cyberwar: a new ‘absolute weapon’? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401-428. https://doi.org/10.1080/01402390.2012.663252

Lin-Greenberg, E. (2019). *Remote Controlled Restraint: The Effect of Remote Warfighting Technology on Crisis Escalation* [Doctoral dissertation]. Columbia University.

Lindsay, J. R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 53-67. https://doi.org/10.1093/cybsec/tyv003

Matania, E., & Tal-Shir, E. (2020). Continuous terrain remodelling: gaining the upper hand in cyber defence. *Journal of Cyber Policy*, 1-17. https://doi.org/10.1080/23738871.2020.1778761

Meernik, J., & Brown, C. (2007). The short path and the long road: Explaining the duration of US military operations. *Journal of Peace Research*, *44*(1), 65-80. https://doi.org/10.1177/0022343307071611

Meyer, P. (2020). Norms of Responsible State Behaviour in Cyberspace. In M. Christen et al. (eds.), *The Ethics of Cybersecurity* (pp. 347-360). Springer, Cham.

Nakashima, E. (2019, June 23). Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers. *The Washington Post.* https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

Osakwe, C., & Umoh, U. E. (2013). Non-Lethal Weapons and Force-Casualty Aversion in 21st Century Warfare. *Journal of Military and Strategic Studies, 15*(1). https://jmss.org/article/view/58087/43712

Quester, G. H. (2002). *Offense and defense in the international system*. Transaction Publishers.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Rottinghaus, B. (2008). Presidential leadership on foreign policy, opinion polling, and the possible limits of “crafted talk”. *Political Communication, 25*(2), 138-157. https://doi.org/10.1080/10584600801985334

Rubenstein, D. (2017). *Nation State Cyber Espionage and its Impacts. Washington University in St. Louis. Internet* (Working Paper). Washington University in St. Louis**.** http://www.cse wustl edu/~jain/cse571-14/ftp/cyber_espionage.pdf

Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy*, *34*(1), 40-63. https://doi.org/10.1080/13523260.2013.771031

Sanger, D. E. (2018, July 27). Russian Hackers Appear to Shift Focus to U.S. Power Grid. *The New York Times*. https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html

Scholz, R. W., Bartelsman, E. J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., ... & Montag, C. (2018). Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. *Sustainability*, *10*(6), 2001. https://doi.org/10.3390/su10062001

Schörnig N. (2014) Liberal Preferences as an Explanation for Technology Choices. The Case of Military Robots as a Solution to the West's Casualty Aversion. In: Mayer M., Carpes M., Knoblich R. (Eds.), *The Global Politics of Science and Technology - Vol. 2. Global Power Shift (Comparative Analysis and Perspectives)*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55010-2_5

Schuurman, B. (2013). Defeated by popular demand: Public support and counterterrorism in three western democracies, 1963–1998. *Studies in Conflict & Terrorism*, *36*(2), 152-175. https://doi.org/10.1080/1057610X.2013.747072

Shandler, R., Gross, M. L., Backhaus, S., Canetti D. (in press). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment. *British Journal of Political Science*.

Shandler, R. (2019). *White Paper: Israel as a Cyber Power (White Paper)*. Israeli National Cyber Bureau. https://doi.org/10.13140/RG.2.2.15936.07681

Shane, P. M. (2012). Cybersecurity Policy as If Ordinary Citizens Mattered: The Case for Public Participation in Cyber Policy Making. *I/S: A Journal of Law and Policy for the Information Society*, 8(2), 433-462. https://heinonline.org/HOL/P?h=hein.journals/isjlpsoc8&i=438

Shields, P. M. (2020). Dynamic Intersection of Military and Society. In A. Sookermany (ed.), *Handbook of Military Sciences* (pp. 1-23) Springer, Cham.

Small, D. A., Lerner, J. S., & Fischhoff, B. (2006). Emotion priming and attributions for terrorism: Americans' reactions in a national field experiment. *Political Psychology*, *27*(2), 289-298. https://doi.org/10.1111/j.1467-9221.2006.00007.x

Small, M. (1996). *Democracy and Diplomacy: The Impact of Domestic Politics in US Foreign Policy, 1789-1994*. JHU Press.

Smith, H. (2005). What costs will democracies bear? A review of popular theories of casualty aversion. Armed forces & society, 31(4), 487-512. https://doi.org/10.1177/0095327X0503100403

Sobel, R. (2001). *Impact of Public Opinion on U.S. Foreign Policy Since Vietnam.* Oxford University Press.

Spielberger, C. D. (1970). *Manual for the state-trait anxiety inventory (Self-evaluation questionnaire)*. Consulting Psychologists Press.

Stein, R. M. (2015). War and revenge: Explaining conflict initiation by democracies. *The American Political Science Review*, *109*(3), 556-573. http://dx.doi.org/10.1017/S0003055415000301

Tidy J. (2020, September 18). Police launch homicide inquiry after German hospital hack. *BBC*. https://www.bbc.com/news/technology-54204356.

Togeby, L. (1994). The gender gap in foreign policy attitudes. *Journal of Peace Research*, *31*(4), 375-392. https://doi.org/10.1177/0022343394031004002

Tomz, M., & Weeks, J. L. (2020). Public opinion and foreign electoral intervention. *American Political Science Review*, *114*(3), 856-873. https://doi.org/10.1017/S0003055420000064

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347-360. https://doi.org/10.1177/0022343313518940

Valeriano, B., & Jensen B. (2019, June 25). How cyber operations can help manage crisis escalation with Iran. *The Washington Post*. https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/

Valeriano, B. G., & Jensen, B. (2019b). The Myth of the Cyber Offense: The Case for Cyber Restraint. *Cato Institute Policy Analysis* (No. 862). https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint?fbclid=IwAR2SHSirl1flE1u-JIQE-4n2rcTDj_LitHHoSF-2QPuE7oDrANAk9FXAXzU

Van Evera, S. (2013). *Causes of war: Power and the roots of conflict*. Cornell University Press.

Vick, A. J. (2015). *Proclaiming Airpower: Air Force Narratives and American Public Opinion from 1917 to 2014* (No. RR-1044-AF). Rand Project Air Force Santa Monica Ca.

Walsh, J. I. (2015). Precision weapons, civilian casualties, and support for the use of force. *Political Psychology*, *36*(5), 507-523. https://doi.org/10.1111/pops.12175

Ward, R. H. (2020). Fewer civilian casualties: Trending toward a constraint on the use of force. *Comparative Strategy*, *39*(1), 29-40. https://doi.org/10.1080/01495933.2020.1702345

Wilcox, C., Hewitt, L., & Allsop, D. (1996). The gender gap in attitudes toward the Gulf War: A cross-national perspective. *Journal of Peace Research*, *33*(1), 67-82. https://doi.org/10.1177/0022343396033001005

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway Books.