

Research paper

Cyberattacks, cyber threats, and attitudes toward cybersecurity policies

Keren L.G. Snider^{*}, Ryan Shandler, Shay Zandani and Daphna Canetti

School of Political Science, University of Haifa, Mount Carmel, Haifa 31905, Israel

^{*}Correspondence address. School of Political Science, University of Haifa, Mount Carmel, Haifa 31905, Israel ; E-mail: kerenlgs@gmail.com

Received 14 May 2020; revised 15 June 2021; accepted 16 August 2021

Abstract

Does exposure to cyberattacks influence public support for intrusive cybersecurity policies? How do perceptions of cyber threats mediate this relationship? While past research has demonstrated how exposure to cyberattacks affects political attitudes, the mediating role played by threat perception has been overlooked. This study employs a controlled randomized survey experiment design to test the effect of exposure to lethal and nonlethal cyberattacks on support for different types of cybersecurity policies. One thousand twenty-two Israeli participants are exposed to scripted and simulated television reports of lethal or nonlethal cyberattacks against national infrastructure. Findings suggest that exposure to cyberattacks leads to greater support for stringent cybersecurity regulations, through a mechanism of threat perception. Results also indicate that different types of exposure relate to heightened support for different types of regulatory policies. People exposed to lethal cyberattacks tend to support cybersecurity policies that compel the government to alert citizens about cyberattacks. People who were exposed to nonlethal attacks, on the other hand, tend to support oversight policies at higher levels. More broadly, our research suggests that peoples' willingness to accept government cybersecurity policies that limit personal civil liberties and privacy depends on the type of cyberattacks to which they were exposed and the perceptions associated with such exposure.

Key words: cyberattacks, cybersecurity, cybersecurity policies, threat perceptions

In recent years, the increase in civilian exposure to cyberattacks has been accompanied by heightened demands for governments to introduce comprehensive cybersecurity policies. These demands peaked in the aftermath of the 2021 Colonial Pipeline and SolarWinds cyberattacks, where the US government's lack of access to cybersecurity information in critical industries wrought havoc on the country's national and economic security. In the aftermath of these attacks, lawmakers and the public exhibited newfound enthusiasm for legislation that would mandate cyberattack reporting by private enterprises—accelerating a regulatory trend that has existed for several years [1]. In 2020, for example, 40 US states and territories introduced more than 280 cybersecurity related bills and resolutions [2, 3]. A similar process has taken place in Europe [4] and in Israel [5, 6].

The public willingness to accept government policies and regulations that limit personal civil liberties and privacy is part of

a delicate tradeoff between security and privacy. In some ways, privacy is seen as an adequate cost of enhanced personal and societal security in the face of novel threats. However, the public has grown increasingly sensitive to the importance of online privacy, and is keenly aware of the ethical, political, legal, and rights-based dilemmas that revolve around government monitoring of online activity and communications [7, 8].

The debate on digital surveillance centers on how and whether authorities should gain access to encrypted materials, and raise key questions concerning the extent of state interference in civic life, and the protection of civil rights in the context of security. Yet what lies at the heart of this willingness to accept government policies and regulations that limit personal civil liberties and privacy via increasing public demand for government intervention in cybersecurity? Does exposure to different types of cyberattacks lead to heightened support for different types of regulatory policies? And does the public

differentiate between interventionist and regulatory forms of cybersecurity policies?

To test these questions, we ran a controlled randomized survey experiment that exposed 1022 Israeli participants to simulated video news reports of lethal and nonlethal cyberattacks. We argue that public support for governmental cybersecurity measures rises as a result of exposure to different forms of cyberattacks, and that perceived threat plays a mediating role in this relationship. More specifically, we propose that exposure to initial media reports about cyberattacks is a key to the exposure effect, since at this time the threat is magnified and the public has minimal information about the identity of the attacker and the type of cyberattack that was conducted. Past events show that in many cases, the public internalizes the details of an attack in its immediate aftermath when media reports are heaviest. While later reports in the days and weeks following an attack will include far more detailed information, the damage by this time has already been done and the public is already scared and alert.

Further to this, we suggest that the literature has erroneously pooled together all cyber regulatory policies under a single banner of cybersecurity. We propose that civilian exposure to different types of cyberattacks leads to increased support for different and specific cybersecurity policies. We therefore differentiate between support for policies that focus on alerting the public in cases of cyberattacks and others that call for oversight of cybersecurity. In examining how exposure to cyberattacks influences support for these specific policy positions, we distinguish between the outcome of cyberattacks—lethal attacks that cause lethal consequences as a first- or second-degree outcome of the attack, versus nonlethal attacks that merely involve financial consequences. This more nuanced breakdown of exposure types and policy options can help officials contend with certain policy debates without the need for a one-size-fits-all policy. For example, reservations expressed by conservative/libertarian scholars who are concerned about government intervention in the commercial marketplace need not disqualify all forms of cybersecurity policy [9]. Likewise, the reservations of those concerned with individual privacy violations need not lead to the denunciation of all policies [10].

To ground this analysis of how the public responds following exposure to both lethal and nonlethal cyberattacks, we apply theories associated with the literature on terrorism and political violence. These theories offer sophisticated mechanisms that explain how individual exposure to violence translates into political outcomes—including demands for government intervention and policymaking. This approach is especially applicable in the digital realm as cyberattacks track a middle ground between technological breakthroughs that constitute tactical developments and new strategic weapons [11]. The consequence of such ambiguity is that civilians who are exposed to digital political threats can only identify the outcomes of the attack—i.e. whether it is a lethal or nonlethal cyberattack—while the motivations and identities of attackers often remain veiled, or at least unsettled. In light of these attributional challenges, and reflecting the fact that the public typically operates in a low-information environment, we refrain from declaring that the cyberattacks that appear in our experimental manipulations are cybercrime, cyberterrorism, cyber-vandalism, or any other type of attack. Rather, we refer to all attacks under the general heading of "cyberattacks," leaving all respondents to react to the attacks in a way that they see as appropriate in light of the severity of the reported outcome.

The most common form of cyberattack is cybercrime. Reports of data breaches resulting from cyberattacks by criminal organizations show a growth of more than threefold between 2011 and 2018 [12]. In the first half of 2019 alone, the United States Treasury Department announced that there had been 3494 successful cyberattacks

against financial institutions resulting in colossal financial losses and the capture of personal information relating to hundreds of millions of people [13]. Cyberattacks executed by terror organizations are a newer phenomenon, albeit one that has captured the popular imagination. While terror organizations predominantly make use of cyberspace for fundraising, propaganda, and recruitment [14, 15], a recent development has been the next-generation capacity of cyber strikes to trigger lethal consequences, be it through first- or second-order effects.¹ We acknowledge that scholars have expressed some skepticism about the likelihood of impending destructive cyberterror incidents [16–18], yet national security officials have regularly predicted that lethal cyberattacks pose a "critical threat" [19]. In the last decade, the nature of this threat has evolved from the earlier depictions of an apocalyptic cyber "pearl harbor" that would ravage modern society from the shadows [20], to a more nuanced understanding that cyberattacks, while still posing a threat to critical infrastructure, are more likely to manifest through targeted strikes. For example, in April 2020, Israel narrowly averted a cyberattack targeting civilian water networks that would have killed scores of civilians by adding chlorine to the water supply [19]. Other physically destructive cyberattacks have caused explosive damage to critical infrastructure [21], while researchers have experimentally verified the ability of malicious digital actors to hack pacemakers and insulin pumps [22]. While the lethal stature of cyberattacks is still developing, these incidents establish the bona fides of this impending threat and the importance of understanding how the public responds to this type of event.

The discussion that follows has four parts. We begin by examining the theory of how exposure to violence translates into policy preferences, with a particular focus on the mediating role of threat perception. Second, we discuss the design of our controlled, randomized experiment that exposes participants to television news reports of lethal and nonlethal cyberattacks. Third, we present our main results and consider various mediation models that pertain to the different regulatory subsets. We conclude by discussing the implications of our findings for the study of cybersecurity and cyber threats more generally.

Exposure to Cyberattacks and Policy Attitudes

Civilians who are exposed to political violence often suffer from feelings of trauma, anxiety, and helplessness in the face of threatening external forces [23–25]. These emotional responses—whether caused by acts of cyber or conventional violence—are known to cause shifts in political attitudes. Research has shown how exposure to conventional terrorism, which targets civilians and disrupts their daily routines, has an impact on individuals' support for attitudes toward peace and compromise with the other [26], political conservatism [27], exclusionism [28] and intragroup relations [29].

Despite the sizeable literature dealing with the effects of exposure to violence, few studies directly investigate the effects of exposure to destructive cyberattacks. This is despite the growing recognition that these threats have become a very tangible part of modern life. In a complex scenario described in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, the authors contemplated how new forms of cyberattacks could be used to "acquire the credentials necessary to access the industrial control system of

¹ Though a DDoS attack, e.g. may not trigger physical casualties, its crippling of emergency services and telecommunications could catastrophically amplify the second- and third-order damage during a physical attack; for more, see Catherine A. Theohary and John W. Rollins, *Cyberwarfare and cyberterrorism: In brief* (Washington, DC: Congressional Research Service, 2015).

a nuclear power plant... with the intent of threatening to conduct cyber operations against the system in a manner that will cause significant damage or death..." [30]. Even more recently, reports have acknowledged how cyberterror attacks could immobilize a country's or region's electrical infrastructure [31], disable military defense systems [32], and even imperil nuclear stability [33]. While there is a difference between capability and intent, and we acknowledge that physically destructive cyber threats have remained scarce until now, understanding how civilians respond to such digital cyberattacks will become particularly important as the threat matures.

Studies that directly investigated exposure to digital political violence found that exposure had significant effects on political behavior and attitudes, akin to exposure to conventional political violence [34, 35]. In a series of exploratory studies regarding the phenomena of cyberterrorism, Gross *et al.* [34, 36] sought to empirically measure the effects of exposure to cyberterrorism under controlled experimental conditions. Their key finding was that exposure to cyberterrorism was severe enough to generate significant negative emotions and cognitive reactions (threat perceptions) at equivalent levels to those of conventional terror acts. Canetti *et al.* [37] found that victims of cyberattacks react by demanding government protection, with psychological distress explaining the relationship between exposure and the demand for government intervention. In a subsequent biologically focused experiment, Canetti *et al.* measured cortisol levels to show how participants who are exposed to cyberterror attacks and experience higher levels of stress are more likely to support hardline retaliatory policies [38].

Building on this foundation, other research has sought to refine a more precise psycho-political mechanism that understands how cyberattacks trigger shifts in political attitudes. Research by Shandler *et al.* [39, 40], e.g. found that only lethal cyberattacks cause political consequences akin to conventional political violence, and that only the emotion of anger explained these shifts.

In the current paper, we aim to add to this emerging body of research by examining the topic of cybersecurity preferences in the aftermath of lethal and nonlethal cyberattacks. While one past study by Cheung-Blunden *et al.* [41] examined how emotional responses to cyber incidents sway cybersecurity preferences, no research has yet attempted to analyze how different types of cyberattacks affect different kinds of cybersecurity policies. As such, we add much needed nuance to the literature.

For the purpose of considering the effects of exposure to cyberattacks, this research focuses on the "outcome" of a cyberattack rather than the "identity" of the perpetrator or the "classification" of the attack. This is necessary for several reasons that relate to the specific characteristics of cyberspace. First, as introduced above, a new class of cyberattack exemplified by the ransomware epidemic has exhibited characteristics of both cybercrime and cyberterror operations, impeding the classification of cyber incidents into simple categories. Second, attribution in cyberspace is fraught with difficulty, and an age of manipulated information complicates the determination of provenance [42–44]. Sophisticated cyber operatives working from anywhere in the world can exploit the principle of anonymity that underlies the Internet infrastructure to hide their identity. Though authorities would be able to quickly identify the identity of an attacker behind any major cyberattack [42], this is essentially impossible for members of the public who are confronted with both structural and technical obstacles that prevent them from rendering an objective judgement about the attack source. This reality of publicly obscured cyber antagonists can be viewed in the timelines of several famous cyber incidents. It took between six months and three years for authorities and private actors to publicly reveal the actors be-

hind the 2017 WannaCry attacks, the 2016 cyber intrusion into the Democratic National Committee's networks, and the 2016 cyberattack against the Bowman Dam in New York [45–47]. While each of these incidents were eventually attributed to an attack source, and the authorities may well have known the identity of the attacker from an early date, we can see that from the perspective of the public, there was a time lag of several months or years before a name was attached to any attack. Third, state involvement in cyberattacks—either as a direct attacker or via proxies—can add substantial background noise to the perception of an attack, raising the specter of interstate war. There is an interesting debate in the literature about whether states may be deemed capable of conducting cyberterrorism—or whether this is a label that can only be applied to nonstate actors. While the literature is still unsettled on this point, Macdonald, Jarvis and Nouri [48] found considerable expert support for the proposition that states can engage in cyberterrorism.

It is for these reasons that we choose to follow the lead of the scholars who are beginning to evaluate responses to cyber threats through the prism that is most readily available for the public—specifically, the outcome variable, or in other words, the lethality of the attack [33]. This focus on outcome rather than attacker is necessary in order to understand the factors that prompt emotional and political responses in the public. While these information asymmetries explain our focus on the *outcome* of the attack rather than the *identity* of the attacker, we acknowledge that the people draw inferences about the identity and motivations of attackers based on prior experiences and political orientation [49]. Liberman and Skitka's vicarious retribution theory [50, 51] demonstrates how the public may impute responsibility to unrelated or symbolically related offenders when the identity of an attacker is unclear. Nonetheless, maintaining the highest standards of ecological validity demands that attribution and attack categorization is absent in initial public reports of cyber incidents.

Under this framework, we hypothesize that:

Hypothesis 1: Exposure to (i) lethal or (ii) nonlethal cyberattacks will lead to greater support for adopting cybersecurity policies compared with people who were not exposed to any cyberattack. In other words, exposure to cyberattacks—lethal (LC) or nonlethal (NLC)—will increase support for adopting cybersecurity policies, as compared with a control group.

Hypothesis 2: People who are exposed to lethal cyberattacks (LC) will exhibit to higher support for adopting cybersecurity policies than people who are exposed to nonlethal cyberattacks (NLC).

The Mediating Role of Threat Perceptions

Civilians are notoriously weak at accurately assessing security threats—a fact that is amplified in the cyber realm due to low cybersecurity knowledge, general cognitive biases in calculating risk, and the distortion of cyber risks by the media, which focuses predominantly on spectacular yet low-likelihood attacks [52–54]. Perceived risk is partly reliant on the scope of the attack to which people are exposed. Victims of cybercrimes (identity theft and cyber bullying) report moderate or severe emotional distress such as anger, fear, anxiety, mistrust, and loss of confidence [55]. The effects of conventional terrorism include post-traumatic stress, depression, and anticipatory anxiety [56, 29]. In both of these cases, threat perception is a common predictor of political attitudes and behavior. Indeed, the best predictor of hostile out-group attitudes is the perceived threat that out-group members will harm members of the in-group, whether physically, economically or symbolically [28, 57, 58]. In many of the studies cited above, threat

perception was found to mediate the relationship between exposure to violence and support for harsh or restrictive policies, especially in conflict-related contexts [27]. Extending this empirical and theoretical evidence to digital political violence suggests that individuals are likely to respond similarly to cyber threats by supporting strong cybersecurity policies through the interceding influence of heightened threat perception.

A set of early studies compared the level of threat evoked by exposure to different forms of cyber threats, identifying key differences in the how cybercrime and cyberterrorism influenced attitudes toward government policy [34, 36]. These studies concluded that direct exposure to cyberterrorism had no effect on support for hardline cybersecurity policies (increased digital surveillance, the introduction of intrusive new regulations), but threat perceptions relating to cyberterrorism successfully predicted support for these policies. Recognizing therefore that threat perception plays a central role in understanding the response to cyberattacks, we predict that

Hypothesis 3: Cyber threat perception will mediate the relationship between individual exposure to cyberattacks and support for cybersecurity policies.

Experimental Method

To test our hypotheses, we conducted a controlled survey experiment that exposed respondents to simulated news reports about major cyberattacks. The experimental manipulation relied on professionally produced original video clips that broadcast feature news reports. The lethal treatment group viewed a feature report discussing several lethal cyberattacks that had taken place against Israeli targets, while the nonlethal treatment group broadcast a collection of stories pertaining to nonlethal cyber incidents (see below for additional details about each manipulation). The control group did not watch any news report.

We utilized the medium of video news reports for our experimental manipulation since experiments in recent years have shown how broadcast videos and media reports of major attacks arouse strong emotions among viewers, which in turn trigger reevaluations of policy positions and political attitudes related to issues of security [35, 59, 60]. The rationale behind these finding can be partly explained by Terror Management Theory, which explains how even indirect exposure to violent acts triggers potent emotional reactions as people confront threats to their mortality [61, 62]. Just as importantly, news reports are a key avenue by which the public learns about major security incidents, and so this method maintains its ecological validity. Each of the groups completed a pre- and post-survey, answering a series of questions about their attitudes to cybersecurity along with relevant sociodemographic information.

Each of the television news reports was presented as an authentic feature story that appeared on Israeli channel 1 television station. The news reports described the global scale of cyber threats facing the public (i.e. two million malicious web sites launch each month and 60 000 new malware programs appear every day at an annual cost to the global economy of 500 billion dollars). The clips were screened in a feature format using on-camera interviews, voiceover and film footage to describe various cyberattacks. To increase the authenticity of the experience, the reports included interviews with well-known Israeli security experts. To mimic the challenges of cyber attribution, the perpetrators of the attacks described in the videos were not identified and were neutrally referred to as cyber operatives. Each video lasted approximately 3 min.

Lethal Cyber Condition—The television news report described various cyberattacks with lethal consequences that had targeted Israel during the previous years. For example, in one of the featured stories, an attack was revealed to have targeted the servers controlling Israel's electric power grid, cutting off electricity to a hospital and causing deaths. In another story, cyber operatives were said to have attacked a military navigation system, altering the course of a missile so that it killed three Israeli soldiers. A third story concerned the use of malware to infect the pacemaker of the Israeli Defense Minister, and a fourth involved the failure of an emergency call to 10 000 military reserve soldiers due to a cyberattack in which foreign agents changed the last digit of the soldiers' telephone numbers in the military database. The video's interviews with well-known figures from Israel's security sector emphasized the life-threatening danger posed by cyberattacks.

Nonlethal Cyber Condition—The television news report revealed various nonlethal cyberattacks that had targeted Israel during recent years. For example, the broadcast explained how mobile phone users are made vulnerable to attackers by installing new games and applications, potentially introducing malware that can later access data like personal messages or financial details. Another example concerned the dangers posed by the Internet of Things and featured a story in which all the major credit cards companies suspended their customer support after hundreds of thousands of citizens were fraudulently charged for food purchases by their smart refrigerators. The Israeli experts in this video emphasized the potential financial damage from cyberattacks.

Participants

The online survey experiment was administered in Israel during September 2015 via the Midgam Survey Panel. One thousand twenty-two participants were randomly assigned to the three groups (lethal condition: $N = 387$; nonlethal condition: $N = 374$; control group: $N = 361$). The experimental sample represents a random cross-section of the Jewish Israeli population. The sample is largely representative of the wider population, and balance checks reveal that the treatment distribution is acceptable. We note that due to data collection constraints, the sample does not include ultra-orthodox (religious) respondents due to difficulties in accessing this subgroup through online methods. The mean age of the participants was 41 ($SD = 14.81$), and gender distribution of 49.96% male and 50.04% female. With respect to political orientation, 44.35% of the sample define themselves as right-wing ($N = 452$), 38.28% themselves as centrist ($N = 390$), and 17.37% as left-wing ($N = 177$) (this reflects the right-wing slant of the Israeli population that has been apparent in recent elections). The distribution of education and income levels was similar across the three groups (Education: $F(2, 1120) = 0.20$, $P < 0.82$; Income: $F(2, 1045) = 0.63$, $P < 0.53$). Sociodemographic characteristics of the participants are presented in Appendix A (Supporting Information), together with experimental balance checks.

Measures

The experiment incorporated three primary variables: the predictor variable (exposure to cyberattacks), the dependent variable (support for cybersecurity policies), and the mediator variable (threat perception). Sociodemographic measures were also collected.

Predictor variable—exposure to cyberattacks

Exposure to cyberattacks was operationalized by random assignment to one of the three experimental treatments described above—lethal cyberattacks/nonlethal cyberattacks/control condition.

Dependent variable: support for cybersecurity policies

Support for cybersecurity policies was examined using twelve questions taken from two scales developed by McCallister and Graves [63, 64]. After separating out one item that reflected a unique form of cybersecurity policy, the remaining items were subjected to a principal component analysis (PCA), which highlighted different aspects of cybersecurity policy. Our criteria for the factor dimension extraction was an eigenvalue greater than one for number of dimensions, and factor loading greater than 0.35, for dimension assignment. We applied the PCA extraction method with the Varimax rotation to construct orthogonal factors [65]. This procedure gave rise to two clearly distinguishable cyber policy dimensions. Following this process, we combined the two remaining items that were excluded due to poor loadings (loading < 0.35) to create a third policy dimension with a high correlation between the items ($r = 0.617$, $P < 0.001$) (see Appendix B in the Supporting Information for the PCA and complete list of the items used to construct each scale). The final three measures of cybersecurity policies reflected the breadth of available policy options, which emphasized different levels of government intervention and oversight strategies. The first of these is cybersecurity prevention policy (CPP); the second is cybersecurity alert policy (CAP); and the third is cybersecurity oversight policy (COP).

The cybersecurity prevention policy dimension (CPP) captures the idea that the state should mandate commercial companies to implement minimum levels of cybersecurity to prevent damage. Respondents were asked questions such as: “should the state compel business owners to protect themselves against cyberattacks?” Cronbach’s α was within an acceptable range at 0.720.

The cybersecurity oversight policy dimension (COP) refers to the notion that the state should directly intervene to offer cyber protection to its citizens and businesses. Relevant questions for this dimension included “should the state protect its citizens from cyberattacks?” Cronbach’s α was within an acceptable range at 0.737.

The cybersecurity alert policy dimension (CAP) relates to the state’s presumed responsibility to ensure citizens are alerted when a hack of a cyberattack is discovered. For example, a related question would ask: “should the state alert citizens after a successful attack on critical infrastructure?” As opposed to the prevention policy dimension that relates to measures that must be taken before a cyberattack, the alert policy focuses on the measures to be taken after an attack. Cronbach’s α was slightly below acceptable range at 0.632. All questions were measured on a scale ranging from 1 (“completely disagree”) to 6 (“completely agree”).

Mediator: perceptions of cybersecurity threats

Threat perception pertaining to cyber threats was gauged using a five-item scale based on studies conducted in the United States [66]. Respondents were asked how concerned they feel about the possibility of an actual threat to their security. Respondents answered questions including: “To what extent does the idea of a cyberattack on Israel affect your sense of personal security?” and “To what extent does a cyberattack on Israel threaten the country’s critical infrastructure?” and the answers ranged from 1 (“not at all”) to 6 (“to a very great degree”). The internal consistency of this measure was very high (Alpha = 0.913).

Control variables

Control variables collected included political ideology (assessed through a self-reported five-point scale ranging from 1 [very conservative] to 5 [very liberal]), age, gender, marital status, religiosity, education, and income.

We also measured and controlled for participants’ past exposure to cyberattacks. To measure this variable, we adapted a four-item scale used to measure exposure to terrorism and political violence [67, 35]. Items included questions that asked the extent to which the respondents, their friends and their family had ever suffered harm or loss from a cyberattack. Similarly to past studies, we did not calculate the internal reliability for past exposure, given that one type of exposure does not necessarily portend another type.

Results**Preliminary analyses**

We begin our analysis by testing the variance between the treatment groups regarding attitudes toward cybersecurity policies, to establish that the experimental conditions produce at least minimal levels of differences in the dependent variables. Hence, we conducted a one-way univariate analysis of variance (ANOVA), in which the different cyber policies were the dependent variables. The results indicated differences between the three groups in support for policies regarding cybersecurity alerts (CAP: $F(2, 1020) = 4.61$, $P < 0.010$). No differences between groups were found in support for cybersecurity prevention policy or cybersecurity oversight policy (CPP: $F(2, 1020) = 1.35$, $P < 0.259$; COP: $F(2, 1020) = 0.94$, $P < 0.39$). We followed the CAP ANOVA analysis with pairwise comparisons using Bonferroni corrections, which revealed that the highest level of support for cybersecurity alerts was expressed by the group exposed to lethal cyberattacks on average, while the other two groups showed lower levels of support for this policy. These results support the conclusion that the differences in cybersecurity policy preferences between the three groups derive from the video stimulus, and not from differences in participants’ sociodemographic characteristics (see Appendix C in the Supporting Information for means and standard deviations of study variables, in all three manipulation groups).

In addition, we tested group differences regarding threat perceptions and found significant differences in threat perceptions between the three groups ($F(2, 1020) = 21.68$, $P < 0.001$). The follow up pairwise comparisons with Bonferroni corrections, revealed that participants in both experimental groups (LC and NLC) expressed higher levels of threat perceptions in comparison to participants in the control group. These analyses provide sufficient preliminary support to conduct more complex analyses that integrate multiple effects in this triangle of exposure to cyberattacks, cyber threat perception, and support for cybersecurity policies.

Mediation analysis

To test hypothesis 3, we ran a path analysis model, i.e. a structural equation modeling with observed indicators only. In this model, the exposure was divided into lethal vs control and nonlethal vs control. More specifically, with regard to the mediation effect, the model structure included two pathways from the experimental conditions to support for cybersecurity policies: From the lethal vs control, and from nonlethal vs control through threat perceptions. The latter variable was expected to mediate the effect condition effects on cyber policy positions as proposed in the theory section.

In order to further investigate the mediation mechanism, we constructed an integrative path analysis model [53]. Running this model enables us to identify direct and indirect effects among all the study variables. We provide modeling results in the following Table 1 and an illustration of the path analysis model in Fig. 1.

Direct effects

Table 1 presents the results of the standardized estimates (beta coefficients) of each experimental group vis-à-vis the control group (i.e. NLC vs control, and LC vs control), perceptions of threat, past exposure to cyberattacks and socio demographic variables—gender, religiosity, education and political ideology—with the three dimensions of cybersecurity policies as the dependent variables. In the pairwise comparison of the experimental groups, which compares the lethal and nonlethal conditions to the control group, we find a larger direct effect in the LC (lethal) group compared with the NLC (nonlethal) group in predicting support for CAP.

A follow-up that compared the two regression weights further confirmed the stronger relative effect of the lethal exposure over the nonlethal exposure (H_2 : NLC-LC = -0.21 (0.10), $P = 0.047$). This demonstrates support for our second hypothesis. People who were exposed to lethal cyberattacks tended to support cybersecurity policies that compel the government and security forces to alert citizens if they have evidence of citizens' computers being hacked or if an act of cyberattack is discovered (CAP) at higher levels than people who were exposed to nonlethal/economic cyberattacks compared with people in the control group.

Interestingly, this trend was reversed for the oversight policies (COP) form of cybersecurity regulation. Here, we identified a significant direct effect wherein exposure to nonlethal cyberattacks led to support for oversight policies (COP) at higher levels than respondents who were exposed to the lethal cyberattacks manipulation or the control group. However, the difference between the two treatment conditions was not significant (NLC-LC = 0.11 (0.08), $P = 0.16$). This indicates that exposure to any kind of cyberattack, lethal or nonlethal, predicts greater support for oversight regulation policies (COP) to the same extent. No direct effect was found between exposure to cyberattacks and support for prevention regulation policies (CPP). By breaking apart this analysis into different dimensions of cybersecurity policies our results reveal how exposure to different forms of cyberattacks contribute to support for distinct types of policy that emphasize oversight or intervention.

Most importantly, results indicate a significant direct effect of threat perceptions on all three dimensions of cybersecurity policy and higher levels of threat perception in the lethal cyber manipulation group compared with the nonlethal cyber manipulation group and the control group.

Mediating effects

Table 2 presents the indirect effects of each of the two treatment conditions in comparison to the control group for the three dimensions of cybersecurity policies—with threat perception as a mediator. The indirect effects are pathways from the independent variable to the policy variables through threat perceptions. In the path analysis model, each dependent variable, i.e. support for particular cybersecurity policies, could have two potential paths, one from the nonlethal condition and the one from the lethal condition. Altogether, six mediation pathways were tested. These indirect outcomes are illustrated in Fig. 1. In the LC group we see a complete mediation effect of threat perceptions and no significant direct effect of exposure on COP support. This means that for those participants who were exposed to the

Table 1: Path: analysis direct effects, standardized estimates

| | Threat (M) Beta (S.E.) [95% CI] | CAP (Y ₁) Beta (S.E.) [95% CI] | COP (Y ₂) Beta (S.E.) [95% CI] | CPP (Y ₃) Beta (S.E.) [95% CI] |
|-------------------------------|--------------------------------------|--|---|---|
| Threat (M) | | | | |
| NLC/Control (X ₁) | 0.163*** (0.034) [0.077, 0.221] | 0.058*** (0.035) [0.088, 0.262] | 0.249*** (0.030) [0.151, 0.275] | 0.273*** (0.032) [0.193, 0.335] |
| LC/Control (X ₂) | 0.207*** (0.033) [0.123, 0.258] | -0.070^* (0.036) [-0.164 , -0.012] | -0.073^* (0.036) [-0.168 , -0.017] | -0.043 (0.037) [0.030, 0.077] |
| Past exposure | | -0.140^{***} (0.035) [-0.230 , -0.080] | -0.024 (0.034) [-0.105 , 0.035] | -0.015 (0.035) [-0.101 , 0.046] |
| Gender | 0.109*** (0.031) [0.028, 0.164] | -0.012 (0.030) [-0.088 , 0.036] | -0.005 (0.030) [-0.083 , 0.035] | 0.016 (0.030) [-0.063 , 0.064] |
| Religiosity | 0.200*** (0.030) [0.125, 0.254] | 0.072* (0.032) [-0.011 , 0.126] | 0.010 (0.031) [-0.070 , 0.060] | 0.050 (0.031) [-0.030 , 0.095] |
| Education | 0.034 (0.031) [-0.051 , 0.085] | -0.044 (0.036) [-0.137 , 0.013] | 0.088** (0.031) [0.004, 0.137] | 0.015 (0.033) [-0.075 , 0.066] |
| Political ideology | -0.049 (0.032) [-0.131 , 0.097] | -0.028 (0.032) [-0.124 , -0.028] | -0.027 (0.031) [-0.104 , 0.022] | -0.033 (0.033) [-0.117 , 0.017] |
| R ² | 0.035 (0.033) [-0.045 , 0.097] | 0.050 (0.032) [-0.025 , 0.106] | 0.027 (0.033) [-0.063 , 0.082] | -0.040 (0.033) [-0.127 , 0.024] |
| | 0.093*** (0.017) | 0.047*** (0.014) | 0.074*** (0.015) | 0.087*** (0.018) |

Standard error in parentheses; * $P < 0.05$, ** $P < 0.01$, *** $P < 0.001$. NLC = non-lethal cyberattack; LC = lethal cyberattack.

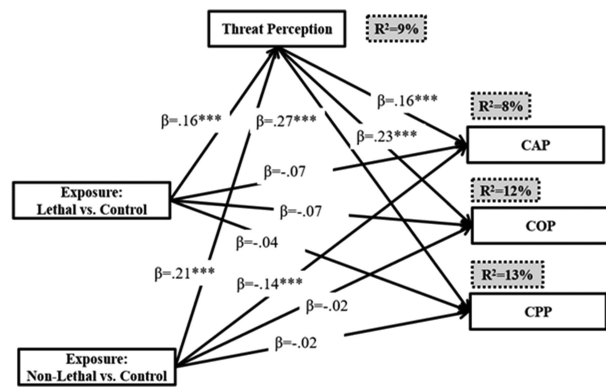


Figure 1: Empirical model results—direct effects of exposure to lethal and nonlethal attack groups vs control group. * $P < 0.05$, ** $P < 0.01$, *** $P < 0.001$.

lethal condition, the actual exposure was not as strong a predictor of policy support as the threat perception associated with the attacks.

In our models predicting CAP, we see a partial mediation effect for both treatment groups, in addition to the direct effect that we described above. We see a larger indirect effect in the LC group than in the NLC group and this was confirmed by a test of difference. This indicates that people who were exposed to lethal cyberattacks reported higher levels of cyber threat perception as compared with people who were exposed to the nonlethal condition, and this heightened threat perception in turn led to more support for various cybersecurity policies.

Support for CAP (i.e. cybersecurity policies whereby the government or relevant organizations are expected to alert citizens if they have evidence of citizens' computers being hacked or an act of cyber-attack being detected) was predicted both by a direct effect of level of exposure to cyberattacks (NLC, LC) and by the mediation of threat perceptions.

Yet our models predicting support for oversight policies (COP) showed a different picture. In the NLC group we see a partial mediation of threat perceptions in addition to the direct effect that we found in the models shown in Table 2. Support for COP (i.e. cybersecurity policies whereby the state should protect the country, organizations, and citizens from cyberattacks through direct government action) was predicted by a direct effect of NLC exposure and by the mediation of threat perceptions in both LC and NLC groups. In the LC group versus the control group, support of COP was predicted only through the mediation perceptions of threat. These results support our third hypothesis regarding the mediating role played by threat perception in predicting COP.

Our models predicting support for prevention policies (CPP) showed a complete mediation effect of threat perception in both experimental treatment groups. No direct effect of exposure on CPP was found, indicating that the mediating mechanism is the best predictor for CPP. Support for CPP (i.e. cybersecurity policies whereby the state compels commercial enterprises to install minimum thresholds of cybersecurity) was predicted by the indirect effect of threat perception.

These results emphasize the central role played by threat perception in predicting support for adopting stringent cybersecurity policies. What is especially noteworthy is that threat perception overrides past experience as the full mediation models indicate. For example, we found that when people are exposed to destructive cyberattacks, the level of perceived threat predicted support for adopting cybersecurity policies that required the state to protect citizens and organi-

zations (COP). Similarly, we found that when it comes to predicting support for prevention policies—threat is the driving force.

In order to complement the indirect effect analyses and test the relative strength of the mediation pathways, we contrasted the indirect effects of the various groups on each policy option. According to the outcome estimates in Table 2, model 3 has a significantly larger mediation effect compared with model 1 (difference = -0.014 ; $0.024 P < 0.001$)², which indicates that within the NLC group, the mediation model is a stronger predictor of support for COP than CAP. In other words, participants who were exposed to the nonlethal condition were more likely to support oversight policies than alert policies.

Discussion

Our findings draw on an experimental design that suggests that exposure to different types of cyberattacks intensifies perceptions of cyber threats and shifts political attitudes in support of stringent cybersecurity policies. We find that exposure to lethal cyberattacks affects individual-level political behavior in a manner akin to conventional terrorism [68–71]. This research was motivated by a desire to better understand what drives individuals to support strong or hardline cybersecurity policies, using Israel as a case study. The findings contribute to this research direction in a number of important ways.

First, exposure to lethal cyberattacks heightens perceptions of cyber threat to a greater degree than nonlethal/economic cyberattacks. Second, as a result of exposure to cyberattacks, respondents were willing to forfeit civil liberties and privacy in exchange for more security. Like conventional terrorism, cyberattacks with lethal consequences harden political attitudes, as individuals tend to support more government oversight, greater regulation of cybersecurity among commercial businesses, and the implementation of strategies to increase public awareness following cyberattacks. Third, our data suggest that in some cases the mere exposure to cyberattack, either lethal or nonlethal, affects the level of support for specific types of cybersecurity policies (stronger support of cybersecurity alert policies among participants in the lethal cyberattack manipulation, and stronger support of cybersecurity oversight policy among participants in the nonlethal cyberattack treatment group). In other cases, threat perception, rather than the exposure to the cyber-events themselves, drive the cognitive effects of cyberattacks on attitudes toward policy (A strong support for COP among the LC group was predicted only through the mediating role of threat perception, and support of CPP, in both manipulation groups was predicted only through a mediated pathway). Finally, we observed differences in the way our mediation model works in relation to different cybersecurity policies.

² We also see a marginal significant effect between mediation 1 and 5 and 2 and 6. The differences between mediation 1 and mediation 5 show mediation 5 (NLC/control-threat-CPP) has a marginal significant larger mediation effect compared with mediation 1 (NLC/control-threat-CAP) (difference = -0.035 ; $0.035 P = 0.073$). This means that within the NLC group the mediation model predicts stronger predicting CPP than CAP. In other words, participants who were exposed to the nonlethal (NLC) condition were more likely to support CPP than CAP. We saw that the CAP is stronger in the LC group. Another marginal significant effect was found between mediation 2 and mediation 6. The differences between mediation 2 and mediation 6 show mediation 6 (LC/control-threat-CPP) has a marginal significant larger mediation effect compared with mediation 2 (LC/control-threat-CAP) (difference = -0.044 ; $0.024 P = 0.062$). This means that within the LC group the mediation model predicts stronger predicting CPP than CAP. In other words, participants who were exposed to the lethal (LC) condition were more likely to support CPP than CAP. We saw a direct effect of LC on CAP.

Table 2: Path: analysis mediation effects, standardized estimates

| | Independent | Mediation | Outcome | Indirect effect (coefficient; S.E. [95% CI]) |
|-------------|-----------------------|-----------|---------|--|
| | CAP | | | |
| Mediation 1 | NLC/Control (X_1) | Threat | CAP | 0.026***; 0.008 [0.010, 0.042] |
| Mediation 2 | LC/Control (X_2) | Threat | CAP | 0.033***; 0.009 [0.015, 0.050] |
| | COP | | | |
| Mediation 3 | NLC/Control (X_1) | Threat | COP | 0.041***; 0.010 [0.020, 0.060] |
| Mediation 4 | LC/Control (X_2) | Threat | COP | 0.052***; 0.011 [0.028, 0.071] |
| | CPP | | | |
| Mediation 5 | NLC/Control (X_1) | Threat | CPP | 0.045***; 0.011 [0.021, 0.066] |
| Mediation 6 | LC/Control (X_2) | Threat | CPP | 0.056***; 0.011 [0.030, 0.077] |

Standard error in parentheses; * $P < 0.05$, ** $P < 0.01$, *** $P < 0.001$. In squared brackets 95% confidence interval with bias correction bootstrapping ($n = 2000$).

The mediation model for the nonlethal condition group participants predicted greater support for cybersecurity policies focusing on oversight rather than policies focusing on alerting the public.

Our study examined public support for three distinct types of cybersecurity policies that we described as prevention policies, alert policies, and oversight policies. Each of these play a role in securing cyberspace, where the uncertainty regarding the form and nature of potential threats calls for a varied array of preventive actions [36, 37]. Each of these policies raises questions about the delicate balancing act between privacy and security demands. In reality, policy approaches are likely to combine several of these elements—yet it behooves us to first consider each of them independently since very little is known about the public knowledge and familiarity with different cybersecurity policies. While preliminary research has looked at public support for cybersecurity preferences in general [41], these have yet to consider the varied approaches to cybersecurity. To that end, in the current paper we tried to simplify the different cybersecurity policies as much as possible based on real-world policies.

Overall, the study provides evidence that exposure to cyberattacks predicts support for cybersecurity policies through the mediating effect of threat perception. Yet our discovery of differential effects depending on the type of cybersecurity policy being proposed adds a new level of nuance that should be probed further in subsequent studies. More so, results indicate that the public worry and concern in the aftermath of cyberattacks leads directly to calls for governmental intervention. This information sheds light on public opinion processes and helps inform our understanding how individuals will likely respond to new cyber threats. It may also help policymakers understand the complex emotions and cognitions evoked by attacks, which can improve policy formulations that respond to the needs of the public.

Future studies should also investigate how fear appeals intervene in this mechanism, and how to motivate people to take cyber threats more seriously in a way that leads to positive behavioral change.

Participants who were exposed to the lethal manipulation supported cybersecurity policies that focus on alerting the public in cases of cyberattacks more than participants in the two other groups. On the other hand, participants who were exposed to the nonlethal manipulation tended to support cybersecurity policies that call for state oversight of cybersecurity. We found no evidence that any type of exposure has a direct effect on support for policies mandating minimum thresholds of cybersecurity in the commercial arena.

One possible explanation for these results is that thus far, cyberattacks have caused economic damage, but lethal cyberattacks that vividly resemble terrorism are a significantly rarer phenomenon. Hence, participants who were exposed to lethal terror cyberattacks supported cybersecurity policies that would alert them and keep them

informed about impending cyber threats. Policies that focus on oversight are perceived as less important during violent terror attacks. On the other hand, exposure to nonlethal cyberattacks, which are typically focused on economic gain, is more common. The economic damage caused by cyberattacks is estimated to reach \$6 trillion by 2021 [72]. As such, participants in the nonlethal manipulation may have regarded cyberattacks causing economic damage as more likely and therefore supported policies that will bolster digital protections.

We note a key condition about the temporal nature of these findings. In analyzing the effect of exposure to cyberattacks, this study focuses on people's immediate response following exposure to cyber threats. Assessing people's short-term responses is valuable as the responses speak to the direction of the political and psychological effects. Yet what is missing from this picture (and beyond the scope of our research design), is the longevity of the response, which speaks to the strength of the effect. If the measured distress and political outcomes swiftly dissipate, then the policy relevance of our findings comes into question.

The literature is split on the question of the temporal durability of attitudinal shifts in the aftermath of major attacks. There is one school of thought that holds that most political effects stemming from political violence or terrorism are fleeting, and that the public is broadly desensitized to political violence [73–75]. Yet a second school of thought suggests that exposure to attacks can trigger prolonged effects and lasting shifts in political and psychological attitudes. Brandon & Silke [76] assert that while the distress triggered by exposure dissipates over time, this is not an instantaneous process. Several longitudinal studies following the Oklahoma bombing and 9/11 found lingering harms, with exposed individuals reporting elevated levels of psychological distress and altered political attitudes for months or years following the event [77–79].

In applying this to the case of cyberattacks, there is insufficient evidence to positively determine the longevity of the political and psychological effects that we identified in our study. We anticipate that the effects will be more than fleeting, since the novelty of cyber threats means that people have yet to undergo any cognitive or emotional desensitization to cyberattacks [80]. However, we acknowledge that this position requires further empirical substantiation in future research.

Conclusion

A central conclusion of this study is that the implementation of cybersecurity regulations should take account of public perception of cyber threats and public exposure to cyberattacks. This position challenges two unspoken yet ubiquitous notions in the field of cybersecurity. First, the formulation of cybersecurity policies—in a manner

akin to national security and espionage discussions—has typically taken place without public input due to the perception that it is a question best left to experts with engineering or national security expertise [81]. Scholars argue that this complete abdication of cybersecurity policy to specialists is a profound mistake, since excluding “the general public from any meaningful voice in cyber policymaking removes citizens from democratic governance in an area where our welfare is deeply implicated” [82]. Functional cybersecurity relies on good practices by the ordinary public, and the failure of cybersecurity awareness campaigns to effectively change behavior may well be linked to the lack of public input in its regulation [81]. Our findings indicate that growing civilian exposure to cyberattacks leads to more defined attitudes toward specific cybersecurity regulations through the mechanism of heightened threat perception. Governments will increasingly need to engage the public as one of the stakeholders in effecting new cyber regulations.

A second conceptual dilemma about the role of public exposure and opinion has to do with the question of whether cybersecurity is a public good deserving of government investment and regulation at all. Much of the field of cybersecurity is dominated by private enterprise, with government involvement taking place in limited ways. Support for government intervention in the realm of cybersecurity is premised on the astronomical public costs of cybercrime, the threat of cyberterror attacks, and the claim of a market failure in the provision of cybersecurity whose negative externalities in the absence of government involvement would cause substantial national damage [83]. A prominent counter-school of thought, resting on a belief that the private market is the most efficient system of allocating economic resources, claims that there is no need for government intervention in the cybersecurity market [84]. These proponents of private sector cybersecurity suggest that the private sector can more effectively achieve cybersecurity outcomes, an assertion that is backed up by the fact that private spending on cybersecurity in 2018 reached USD \$96 billion [85]. This raises the question of how civilian exposure to cyberattacks and the subsequent support for cybersecurity regulation can translate to real outcomes if the market responds to both public and private interests, which take account of public opinion and civilian threat perception in different ways.

Seeing that cyber threats are continuously evolving, there are opportunities to expand and consolidate this research in future studies. In the current article, we focus on the effect of exposure to lethal and nonlethal cyberattacks on support for different types of cybersecurity policies among Israeli participants. Yet despite this singular geographic focus, the results offer lessons that can be applied widely. Like several other Western countries, Israel has been repeatedly exposed to publicly reported cyberattacks on critical infrastructure. And, similarly to American and some European countries, Israel has high levels of Internet penetration and publicly renowned levels of cybersecurity readiness to deal with such attacks. Past studies that examined public perceptions of cyber threats have replicated the findings across multiple countries. Shandler *et al.* [80] found that psychological responses to internalized reports of cyberattacks explains support for military retaliation, and that this mechanism applies similarly in Israel, the United States, and England. Though requiring additional research, the evidence suggests that cyber threats operate via an underlying psycho-political mechanism that transcends national borders. In fact, the effects of cyberattacks may prove weaker in Israel than elsewhere as the constant exposure among Israelis to political violence places digital violence in the context of a political struggle that has, in many ways, fixed and acceptable costs [34]. Therefore, we believe that an Israeli sample offers major advantages in understanding the effects of cyberattacks among other Western nations. Nonetheless, we

encourage future studies to corroborate these findings in different settings.

A second area where our findings could benefit from additional research relates to the nature of the media exposure. In this study, we exposed respondents to “initial” media reports about major cyberattacks where there is minimal information pertaining to the identity of the attacker and the type of attack that was conducted. While this in many ways reflects the reality of media reports about cyberattacks, it does not discount that journalists will sometimes make inferences about the details of an attack, and that later reports in the days and weeks following an attack will include far more detailed information. More so, this article bears implications for a wide literature beyond the political violence discipline. The public discussion regarding digital privacy and surveillance has spurred crucial new research on the dynamics of digital insecurity. In communications and media studies, for example, scientists are focusing on information-age warfare via different social media platforms, and early results show that citizens are as active in correcting disinformation online as they are in spreading disinformation [86, 87]. The debate in the field of business management is also developing as it focuses on consumer expectations surrounding information technology and big data, as well as on the roles and responsibilities of public and private actors in securing personal data [88, 89].

Cyber threats are a critical and growing component of national security. As this threat continues to grow all over the world, both in its public perception and in the true scope of the threat, the need to implement strong cybersecurity regulations will grow as well. Our findings indicate that particular forms of exposure to cyberattacks can contribute to support for various types of cybersecurity legislation and contribute to their public legitimacy. This is especially important since the introduction of these regulations constitutes a sacrifice of civil liberties, a sacrifice that citizens are prone to support only under particular conditions.

Supplementary Data

Supplementary data available at *Cybersecurity Journal* online.

References

1. Geller E, Matishak M. A federal government left ‘completely blind’ on cyberattacks looks to force reporting. *Politico* 2021. <https://www.politico.com/news/2021/05/15/congress-colonial-pipeline-disclosure-488406> (10 August, 2021, date last accessed).
2. Cybersecurity legislation 2020. NCSL. <https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx> (17 October 2020, date last accessed).
3. US state cybersecurity regulation more than doubled in 2017, while federal regulation waned. *BusinessWire*. <https://www.businesswire.com/news/home/20180129005238/en/State-Cybersecurity-Regulation-Doubled-2017-Federal-Regulation> (29 January 2018, last accessed).
4. Kasper A. EU cybersecurity governance: stakeholders and normative intentions towards integration. In: Harwood M, Moncada S, Pace R (eds). *The Future of the European Union: Demisting the Debate*. Msida: Institute for European Studies, 2020, 166–85.
5. Israel National Cyber Directorate (INCD). <https://www.gov.il/en/departments/about/newabout> (1 February 2021, date last accessed).
6. Ochoa CS, Gadinger F, Yildiz T. Surveillance under dispute: conceptualizing narrative legitimization politics. *Eur J Int Secur* 2021;6:210–32.←
7. Flyverbom M, Deibert R, Matten D. The governance of digital technology, big data, and the internet: new roles and responsibilities for business. *Bus Soc* 2019;58:3–19.←
8. Rosenzweig P. The alarming trend of cybersecurity breaches and failures in the U.S. government. The Heritage Foundation.

- <https://www.heritage.org/defense/report/the-alarming-trend-cybersecurity-breaches-and-failures-the-us-government-continues> (17 April 2020, last accessed).
9. Lee JK, Chang Y, Kwon HY. *et al.* Reconciliation of privacy with preventive cybersecurity: the bright internet approach. *Inf Syst Front* 2020;22:45–57.
 10. Nye JS. Nuclear lessons for cyber security? *Strateg Stud Q* 2011;5:18–38.
 11. Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). *Statista*. <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed> (26 February 2019, last accessed).
 12. For big banks, it's an endless fight with hackers *The Business Times*, 30 July 2019. <https://www.businesstimes.com.sg/banking-finance/for-big-banks-it%E2%80%99s-an-endless-fight-with-hackers>
 13. Nye JS, Jr. *Cyber Power*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.
 14. Stohl M. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? *Crime Law Soc Change* 2006;46:223–38.
 15. Lawson ST. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. New York: Routledge, 2019.
 16. Valeriano B, Maness RC. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.
 17. Lawson S. Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *J Inf Technol Polit* 2013;10:86–103.
 18. Israeli cyber chief: Major attack on water systems thwarted. 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 (28 May 2020, last accessed).
 19. Panetta warns of dire threat of cyberattack on U.S. New York Times. (October 11, 2012). <https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>
 20. Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res* 2019;54:971–80.
 21. Zetter K. A cyber attack has caused confirmed physical damage for the second time ever. *Wired* 2015. <http://www.wired.com/2015/01/german-steel-mill-hack-destruction>. (April 2020, date last accessed).
 22. Hobfoll SE, Canetti-Nisim D, Johnson RJ. Exposure to terrorism, stress-related mental health symptoms, and defensive coping among Jews and Arabs in Israel. *J Consult Clin Psychol* 2006;74:207–18.
 23. Halperin E, Canetti-Nisim D, Hirsch-Hoefler S. The central role of group-based hatred as an emotional antecedent of political intolerance: Evidence from Israel. *Polit Psychol* 2009;30:93–123.
 24. Bar-Tal D, Halperin E, de Rivera J. Collective emotions in conflict situations: societal implications. *J Soc Issues* 2007;63:441–60.
 25. Hirsch-Hoefler S, Canetti D, Rapaport C. *et al.* Conflict will harden your heart: exposure to violence, psychological distress, and peace barriers in Israel and Palestine. *Br J Polit Sci* 2016;46:845–59.
 26. Bonanno GA, Jost JT. Conservative shift among high-exposure survivors of the September 11th terrorist attacks. *Basic Appl Soc Psychol* 2006;28:311–23.
 27. Canetti-Nisim D, Ariely G, Halperin E. Life, pocketbook, or culture: the role of perceived security threats in promoting exclusionist political attitudes toward minorities in Israel. *Polit Res Q* 2008;61:90–103.
 28. Zeitzoff T. Anger, exposure to violence, and intragroup conflict: a “lab in the field” experiment in southern Israel. *Polit Psychol* 2014;35:309–35.
 29. Schmitt N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
 30. Russian hackers appear to shift focus to U.S. power grid. *The New York Times*, 27 July 2018. 2018
 31. Aucsmitth D. Disintermediation, Counterinsurgency, and Cyber Defense. 2016, Available at SSRN 2836100. doi: 10.1093/cybsec/tyw018, (10 August, 2021 last accessed).
 32. Gartzke E, Lindsay JR. Thermonuclear cyberwar. *J Cybersecur* 2017;3:37–48.
 33. Gross ML, Canetti D, Vashdi DR. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *J Cybersecur* 2017;3:49–58.
 34. Backhaus S, Gross ML, Waismel-Manor I. *et al.* A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychol Behav Soc Netw* 2020;23:595–603.←
 35. Gross ML, Canetti D, Vashdi DR. The psychological effects of cyberterrorism. *Bull At Sci* 2016;72:284–91.
 36. Canetti D, Gross ML, Waismel-Manor I. Immune from cyber-fire? The psychological & physiological effects of cyberwar. In: Allhoff F, Henschke A, Strawser BJ (eds). *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press, 2016, 157–76.
 37. Canetti D, Gross ML, Waismel-Manor I. *et al.* How cyberattacks terrorize: Cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychol Behav Soc Netw* 2017;20:72–7.
 38. Shandler R, Gross MG, Backhaus S. *et al.* Cyber terrorism and public support for retaliation: a multi-country survey experiment. *Br J Polit Sci* 1–19, 2021. DOI: 10.1017/S0007123420000812.
 39. Rosenzweig P. Cybersecurity and public goods, The public/private ‘partnership’. In: Berkowitz P (ed). *Emerging Threats in National Security and Law*. Stanford: Hoover Institution, Stanford University, 2011, 1–36.
 40. Cheung-Blunden V, Cropper K, Panis A. *et al.* Functional divergence of two threat-induced emotions: fear-based versus anxiety-based cybersecurity preferences. *Emotion* 2017;19:1353–65.
 41. Jardine E, Porter N. Pick your poison: the attribution paradox in cyberwar. . 2020, <https://osf.io/preprints/socarxiv/etb72/>.
 42. Rid T, Buchanan B. Attributing cyber attacks. *J Strateg Stud* 2015;38:4–37.
 43. Clark DD, Landau S. Untangling attribution. *Harvard National Secur J* 2011;2:323–52.
 44. Alraddadi W, Sarvotham H. A comprehensive analysis of WannaCry: technical analysis, reverse engineering, and motivation. <https://docplayer.net/130787668-A-comprehensive-analysis-of-wannacry-technical-analysis-reverse-engineering-and-motivation.html>, (17 April 2020, last accessed).
 45. Romanosky S, Boudreaux B. Private-sector attribution of cyber incidents: benefits and risks to the US government. *Int J Intell CounterIntelligence* 2020;0:1–31.
 46. Baezner M. Iranian cyber-activities in the context of regional rivalries and international tensions. *ETH Zurich* 2019:1–37.
 47. Macdonald S, Jarvis I, Nouri L. State cyberterrorism: a contradiction in terms? *J Terrorism Res* 2015;6:62–75.
 48. Canetti D, Gubler J, Zeitzoff T. Motives don't matter? Motive attribution and counterterrorism policy. *Polit Psychol* 2021;42:483–99.
 49. Liberman P, Skitka LJ. Revenge in US public support for war against Iraq. *Public Opin Q* 2017;81:636–60.
 50. Liberman P, Skitka LJ. Vicarious retribution in US public support for war against Iraq. *Secur Stud* 2019;28:189–215.
 51. Kostyuk N, Wayne C. The microfoundations of state cybersecurity: cyber risk perceptions and the mass public. *J Glob Secur Stud* 2021;6:ogz077.
 52. Gomez MA. Past behavior and future judgements: seizing and freeing in response to cyber operations. *J Cybersecur* 2019;5:1–19.
 53. Gomez MA, Villar EB. Fear, uncertainty, and dread: cognitive heuristics and cyber threats. *Polit Gov* 2018;6:61–72.
 54. Harrell E, Langton L. *The Victims of Identity Theft*, 2012. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2013. <https://www.bjs.gov/content/pub/pdf/vit12.pdf>
 55. Sinclair SJ, Antonius D. *The Psychology of Terrorism Fears*. Oxford: Oxford University Press, 2012.
 56. Quillian L. Prejudice as a response to perceived group threat: population composition and anti-immigrant and racial prejudice in Europe. *Am Sociol Rev* 1995;60:586–611.
 57. Ben-Nun Bloom P, Arikian G, Lahav G. The effect of perceived cultural and material threats on ethnic preferences in immigration attitudes. *Ethn Racial Stud* 2015;38:1760–78.

58. Shoshani A, Slone M. The drama of media coverage of terrorism: emotional and attitudinal impact on the audience. *Stud Confl Terror* 2008;31:627–40.←
59. Huddy L, Smirnov O, Snider KL. *et al.* Anger, anxiety, and selective exposure to terrorist violence. *J Confl Resolut* 2021;00220027211014937.←
60. Greenberg J, Pyszczynski T, Solomon S. The causes and consequences of a need for self-esteem: a terror management theory. In: *Public Self and Private Self*. New York, NY: Springer, 1986, ←212–189.
61. Hall BJ, Hobfoll SE, Canetti D. *et al.* The defensive nature of benefit finding during ongoing terrorism: an examination of a national sample of Israeli Jews. *J Soc Clin Psychol* 2009;28:993–1021.←
62. Canetti D, Hall BJ, Rapaport C. *et al.* Exposure to political violence and political extremism. *Eur Psychol* 2013; 18:263–72
63. McCallister E. *Guide to Protecting the Confidentiality of Personally Identifiable Information*. Darby: Diane Publishing, 2010.
64. Graves J, Acquisti A, Anderson R. Experimental measurement of attitudes regarding cybercrime. In: *13th Annual Workshop on the Economics of Information Security* 2014; Pennsylvania State University.←
65. Huddy L, Feldman S, Capelos T. *et al.* The consequences of terrorism: disentangling the effects of personal and national threat. *Polit Psychol* 2002;23:485–509.
66. Hefetz A, Liberman G. The factor analysis procedure for exploration: a short guide with examples. *Cult Educ* 2017;29:526–62.
67. Muthén LK, Muthén BO. *MPlus: Statistical Analysis with Latent Variables: User's Guide*. Muthén & Muthén, Los Angeles, CA, 2012.
68. Galea S, Ahern J, Resnick H. *et al.* Psychological sequelae of the September 11 terrorist attacks in New York City. *N Engl J Med* 2002;346: 982–7.
69. Canetti-Nisim D, Halperin E, Sharvit K. *et al.* A new stress-based model of political extremism: personal exposure to terrorism, psychological distress, and exclusionist political attitudes. *J Confl Res* 2009;53:363–89.
70. Canetti D, Snider KLG, Pedersen A. *et al.* Threatened or threatening? How ideology shapes asylum seekers' immigration policy attitudes in Israel and Australia. *J Refug Stud* 2016;29:583–606.
71. Morgan S. Cybersecurity Ventures predicts cybercrime will cost the world in excess of \$6 trillion annually by 2021. Cybercrime Magazine. 2017 <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/> (11 May 2020, date last accessed).
72. Yakter A, Harsgor L. Long-term change in conflict attitudes: a dynamic approach. ←2021. http://liran.harsgor.com/wp-content/uploads/2021/07/YakterHarsgor_2021_Long-term-conflict.pdf
73. Brouard S, Vasilopoulos P, Foucault M. How terrorism affects political attitudes: France in the aftermath of the 2015–2016 attacks. *West Eur Polit* 2018;41:1073–99.
74. Castanho Silva B. The (non)impact of the 2015 Paris terrorist attacks on political attitudes. *Pers Soc Psychol Bull* 2018;44:838–50.
75. Brandon SE, Silke AP. Near- and long-term psychological effects of exposure to terrorist attacks.← In: Bongar B, Brown LM, Beutler LE al. *et* (eds). *Psychology of Terrorism*. Oxford: Oxford University Press 2007, 175–93.
76. Pfefferbaum B, Nixon SJ, Krug RS. *et al.* Clinical needs assessment of middle and high school students following the 1995 Oklahoma City bombing. *Am J Psychiatry* 1999;156:1069–74.←
77. Galea S, Vlahov D, Resnick H. *et al.* Trends of probable post-traumatic stress disorder in New York City after the September 11 terrorist attacks. *Am J Epidemiol* 2003;158:514–24.←
78. Landau MJ, Solomon S, Greenberg J. *et al.* Deliver us from evil: the effects of mortality salience and reminders of 9/11 on support for President George W. Bush. *Pers Soc Psychol Bull* 2004;30:1136–50.←
79. Nussio E. Attitudinal and emotional consequences of Islamist terrorism. Evidence from the Berlin attack. *Polit Psychol* 2020;41:1151–71.←
80. Bada M, Sasse AM, Nurse JRC. Cyber security awareness campaigns: why do they fail to change behaviour?In: *International Conference on Cyber Security for Sustainable Society*, Global Cyber Security Capacity Centre. 2015, 1–11.
81. Shane PM. Cybersecurity policy as if 'ordinary citizens' mattered: the case for public participation in cyber policy making. *SSRN Electron J* 2012;8:433–62.
82. Shandler R. White paper: Israel as a cyber power. 2019,DOI: 10.13140/RG.2.2.15936.07681.
83. Gartner forecasts worldwide security spending will reach \$96 billion in 2018, up 8 percent from 2017. Gartner. <https://www.gartner.com/newsroom/id/3836563> (1 August 2019, date last accessed).
84. Shandler R, Gross ML, Canetti D. A fragile public preference for using cyber strikes: evidence from survey experiments in the United States, United Kingdom and Israel. *Contemp Secur Policy* 2021;42:135–62
85. Prier J. Commanding the trend: social media as information warfare. *Strateg Stud Q* 2017;11:50–85.←
86. Golovchenko Y, Hartmann M, Adler-Nissen R. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. *Int Aff* 2018;94:975–94.←
87. Belk RW. Extended self in a digital world. *J Consum Res* 2013;40:477–500.
88. West SM. Data capitalism: redefining the logics of surveillance and privacy. *Bus Soc* 2019;58:20–41.
89. Cahane A. The new Israeli cyber draft bill: a preliminary overview. CSRCL. 2018. <https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill>. (10 August, 2021, date last accessed).