

# The hidden threat of cyber-attacks – undermining public confidence in government

Ryan Shandler & Miguel Alberto Gomez

**To cite this article:** Ryan Shandler & Miguel Alberto Gomez (2023) The hidden threat of cyber-attacks – undermining public confidence in government, Journal of Information Technology & Politics, 20:4, 359-374, DOI: [10.1080/19331681.2022.2112796](https://doi.org/10.1080/19331681.2022.2112796)

**To link to this article:** <https://doi.org/10.1080/19331681.2022.2112796>



© 2022 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 18 Aug 2022.



Submit your article to this journal [↗](#)



Article views: 5518



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 9 View citing articles [↗](#)

## The hidden threat of cyber-attacks – undermining public confidence in government

Ryan Shandler  and Miguel Alberto Gomez 

### ABSTRACT

This paper argues that the primary threat posed by cyber-attacks is not cataclysmic physical destruction - but rather more insidious societal risks such as reduced trust in government. To test this claim, we collect and analyze survey data in the immediate aftermath of a ransomware attack against a Düsseldorf hospital ( $n = 707$ ). We find that exposure to cyber-attacks significantly diminishes public confidence among segments of the population who are exposed to the attack. Cyber-attacks exploit particular qualities of cyberspace that are directly tied to matters of public confidence, causing a precipitous drop in public trust. Second, we identify the psychological mechanism underpinning this effect, with anger and dread intervening in countervailing directions. Feelings of anger triggered by exposure to cyber-attacks amplify public confidence, while the more potent feeling of dread reduces confidence. Our findings verify that governments cannot rely on a unifying social-cohesion effect following cyber-attacks since the public is liable to perceive the authorities as incapable of defending against future threats. We conclude by discussing why escalating cyber-threats can cause severe social upheaval and reduce trust in democratic institutions, and discuss what constitutes exposure to the new generation of attacks in cyberspace.

### KEYWORDS

Cyber-attacks; public confidence; anger; dread; ransomware; trust in government

### Introduction

Exaggerated depictions of cyber-Armageddon have long abounded. Yet the long-predicted flood of physically catastrophic cyber-attacks that threatened to shake countries to their core never eventuated. These attacks may still be forthcoming, but the more likely scenario is that cyber-war will not take place, cyber-attackers will continue to encounter challenges in levying physical destruction, and cyber techniques are poorly suited to the task of fomenting terror (Gartzke, 2013; Rid, 2012; Valeriano & Maness, 2015; Lindsay, 2013). Even so, we do not belittle the threat posed by mounting cyber-attacks. If we look beyond the lack of enduring physical consequences, cyber-attacks can still levy tremendous damage by undermining societal cohesion and trust in government institutions, traumatizing civilians, and dividing communities. According to Schneider (2021, 2022), cumulative minor cyber-attacks collectively eat away at the heart of our digital communities and target the soft underbelly of democratic societies. According to this perspective, the primary threat of cyber-attacks is not cataclysmic physical destruction but rather more insidious, long-term, psychological

and societal harms – such as diminishing public trust in government (Maschmeyer, 2022).

Despite increasing acceptance of this subtler view of the insidious nature of cyber threats, there remains a lack of empirical substantiation. An initial wave of controlled experimental research sought to examine how exposure to cyber-attacks influences public demands for retaliation (Leal & Musgrave, 2022; Shandler et al., 2022), confidence in government leadership (Gross, Canetti, & Vashdi, 2017), and support for adopting cybersecurity regulation (Cheung-Blunden, Cropper, Panis, & Davis, 2019; Kostyuk & Wayne, 2021; Snider, Zandani, Shandler, & Canetti, 2021). However, while the conclusions have proven promising, scholars continue to cast doubt on the findings' external validity due to the difficulty of recreating credible cybersecurity incidents in controlled settings (Gomez, 2019; Spring, Moore, & Pym, 2017).

In an attempt to offer real-world validation of how cyber-attacks influence public opinion and political attitudes, we report the results of a study conducted in the immediate aftermath of a ransomware attack in Düsseldorf, Germany. On

the night of September 9, 2020, a ransomware attack disrupted operations at a hospital, scrambling medical data and rendering computer systems inoperable. In the week following heavy media reporting of the incident, we surveyed 707 residents of North Rhine-Westphalia.<sup>1</sup> By measuring people's exposure to the incident, and applying a propensity score matching technique to overcome confounding effects, we demonstrate how the cyber-attack triggered strong emotional responses which, in turn, undermined public confidence in the government's ability to defend against future attacks. This outcome demonstrates that even if a cyber-attack fails to cause major physical destruction, it can still levy far-reaching societal consequences.

In reaching this conclusion, we limit our focus to the political consequences of *degradative* cyber-attacks. Degradative cyber-attacks refer to attacks that degrade or destroy some aspect of a target's networks, operations, or functions (Valeriano, Jensen, & Maness, 2018). This class of attack needs to inflict physical damage to systems and equipment or degrade their future use, and must cause some physical effect in the real world – either directly or indirectly. Examples of degradative cyber-attacks include the infamous Colonial Pipeline cyber-attack in 2021, which indirectly inhibited gas flow throughout the United States. Other examples include cyber-attacks against water companies, railway infrastructure, and the Dusseldorf hospital attack described above. What is common throughout these examples is that they go beyond the mere manipulation of data or theft of information, and generate tangible consequences outside of cyberspace. We limit the scope conditions of our theory since cyber-attacks are now so varied that it is a mistake to aggregate all cyber-attacks into a homogenous cluster. Furthermore, minor cyber-attacks are so pervasive that the public has begun to demonstrate a measure of resilience to their effects.

Our findings offer three main contributions. First, the results provide strong evidence that exposure to cyber-attacks lowers the public's confidence in their government. This corroborates earlier findings into the effects of cyber-attacks on public opinion, and confirms that cyber incidents manifest different effects than conventional violence,

necessitating the adoption of unique digital-era political models. Second, we identify the psychological mechanism underlining these effects, with anger and dread intervening in countervailing directions. Feelings of anger amplify confidence, while the more potent feeling of dread reduces confidence. Third, these findings highlight the value of real-world and externally valid research on cyber-attacks. Until now, no other research has succeeded in conducting empirical studies that examine the effects of exposure to cyber threats in a natural setting due to the difficulty in operationalizing the concept of exposure and the dearth of relevant case studies.

### ***Exposure to cyber-attacks and public confidence***

The public perceives the government as ultimately responsible for defending critical infrastructure and public institutions against cyber-attacks (de Bruijn & Janssen, 2017). Inevitably, the reality is far more nuanced, with private institutions, software companies, and personnel all playing a role in guarding against damaging digital intrusions (de Bruijn & Janssen, 2017). Even with the most sophisticated cybersecurity policies, a single user ignoring security edicts and clicking on an infected link can facilitate a damaging attack. Nevertheless, the public views the government as responsible for cybersecurity, and degradative cyber-attacks against public institutions cause the public to reassess their level of confidence in the government's ability to confront this pervasive scourge.<sup>2</sup>

Depending on the motivations of an attacker, sowing fear and eroding public confidence in the ability of governments to protect their citizens may be the primary objective of an attack (cyber-terrorism), or it may be an inadvertent second-order effect (cyber-crime, cyber-espionage and cyber-vandalism). For this analysis, we define public confidence as *a subjective evaluation of the ability of governments, leaders, and national security services to prevent and mitigate attacks and maintain a functioning state* (Baldwin, Ramaprasad, & Samsa, 2008).<sup>3</sup>

In examining the effect of exposure to cyber-attacks, we draw from a bedrock theory in the study of public opinion, the rally 'round the flag effect, which posits that foreign attacks against

domestic targets *heighten* public support in the short-term for leaders (Huddy, Feldman, Taber, & Lahav, 2005; Mueller, 1973) and government institutions (Dinesen & Jæger, 2013). This effect is not necessarily associated with a rational assessment of governmental competence in the face of external threat. Rather, it is driven by a psychological need for security in an environment of uncertainty which is met by putting aside societal differences and banding together against a common enemy.

A spate of cyber-attacks in recent years has rejuvenated questions about the applicability of this theory in cyberspace, with doubts cast on the ability of such incidents to trigger a spike in public confidence (Kertzer et al., 2021). The reason for this skepticism is that cyber-attacks exploit qualities of cyberspace that are directly tied to matters of public trust. One quality is the difficulty of attribution in cyberspace. The public is typically unable to verify the identity of cyber-attackers. Even in cases where the authorities identify the perpetrator, ambiguity often exists regarding the veracity of the information (Egloff, 2019). The lack of confidence vis-à-vis the attacker's identity heightens threat perception due to the omniscience associated with cyber operatives (Dunn Cavelty, 2012). Moreover, in contrast with conventional political violence or terrorism, the public is continuously exposed to an increasing quantity of high-profile attacks. While severe conventional attacks are rare enough to spark a rally event, an epidemic of cyber-attacks is likely to encourage the belief that the security forces cannot combat this phenomenon.

Another distinct quality of cyber attacks is the overwhelming sense of helplessness they engender. When it comes to conventional violence – like rockets or knife attacks – the public understands how to protect themselves by going to a bomb shelter or avoiding dark alleys. However, in cyberspace, the sheer complexity of the domain arouses a sense of helplessness in the face of seemingly omnipotent attackers, which can, in turn, alter people's response patterns and influence public confidence (Bada & Nurse, 2020; Kostyuk & Wayne, 2021). In this way, cyber-attacks arouse different levels of emotional distress and generate discrete political outcomes compared to conventional attacks, raising the prospect of distinctive logic of

violence in cyberspace (Shandler, Snider & Canetti, 2022).

The empirical research on the effects of cyber-attacks on public confidence is, at present, inconclusive. One study by Gross et al. (2017) exposed participants to simulated video clips depicting cyber-attacks against critical infrastructure, concluding that conventional terrorism and cyber-terrorism produce comparable effects on the public's confidence in the government's ability to defend against future attacks. By contrast, other research demonstrated that personal exposure to cyber-attacks heightens people's belief that they will be targeted again in the future, with prospective government intervention viewed as futile (Kostyuk & Wayne, 2021). Following this, we propose that:

**Hypothesis 1:** *Exposure to cyber-attacks against public institutions will lower public confidence in government.*

### ***The role of emotions in cyber attacks***

The study of emotions notes that affective responses to violent incidents elicit coping behaviors that drive shifts in political attitudes (Canetti, 2017). Invoking specific emotions cause corresponding effects on attitudes, behavior, and decision making. Even emotions with similar positive or negative valence (e.g., sadness, anxiety, and anger) can cause distinct and contradictory outcomes (Lerner, 2001). We know that responses to violent incidents characterized by feelings of fear or anxiety lead to increased support for protective policies (such as increased funding for security forces) as a method of reducing the perceived threat. By contrast, public sentiment characterized by anger amplifies support for aggressive retaliatory action. As research into emotions proliferates, it is now widely acknowledged that a comprehensive understanding of the political effects stemming from public events requires us to incorporate emotional responses into our models, especially when the events include out-group threats. For instance, research demonstrates how emotional distress resulting from exposure to political violence undermines one's sense of security (Huddy et al., 2005;

Neria, DiGrande, & Adams, 2011), increases support for hard-line policies (Bleich, 2003; Bonanno & Jost, 2006), fosters a rightward shift in security and privacy issues (Janoff-Bulman, 1992), and leads to increased demands for military action against perpetrators (Canetti, 2013; McDermott, 2010).

Yet how does the literature on emotions and conventional violence translate to incidents in cyberspace? Scholars note several distinguishing qualities of cyberspace that activate distinct emotional responses that are likely to alter the aforementioned mechanisms. For example, the portrayal of cyber-attacks as an existential threat can amplify emotional responses due to the mystique associated with near-omniscient cyber actors (Dunn Cavelty, 2019; Jarvis, Macdonald, & Whiting, 2017; Lawson, 2019). Relatedly, Gomez and Villar (2018) and Kostyuk and Wayne (2021) observe that the public's lack of technical sophistication in the cyber domain awakens feelings of uncertainty and dread. Finally, the attribution dilemma in cyberspace gives rise to unique dynamics among observers (Kello, 2013). This dilemma refers to a reality wherein cyber actors operate in an environment of anonymity, and where the public is typically unable to verify the identity of an attacker (Egloff, 2019; Egloff & Wenger, 2019). The absence of knowledge about an attacker's identity can either aggravate risk perception (Kaminska, 2021; Dunn Cavelty, 2012) or leave victims feeling perplexed and confused (Gartzke, 2013).

Based on these studies, we identify three recurring emotions that are likely to be aroused in the aftermath of cyber-attacks, and in turn, drive policy preferences. These are *anger*, *dread*, and *anxiety*. While other emotions such as sadness, confusion, or disgust will undoubtedly be felt, these tend to be less consequential in shifting political attitudes. There is little evidence to suggest that these feelings will mediate exposure to cyber violence and public confidence.

### Anger

The feeling of anger is “an emotional state that consists of feelings that vary in intensity, from mild irritation or annoyance to intense fury and rage” (Spielberger et al., 1995). The passion and fury that we associate with anger are driven by a desire to correct perceived injustices or slights,

which is why anger is considered a particularly active emotion that compels people to take action (Fischer & Roseman, 2007; Halperin, Russell, Dweck, & Gross, 2011). In the cybersecurity literature, anger is used to explain how exposure to attacks leads to heightened militancy, support for retaliation against the perpetrator, and support for adopting strict cybersecurity policies (Shandler et al. 2022).

### Dread

We define dread as the apprehension of the negative consequences of an event. Incidents that are uncertain and subjectively perceived to give rise to potentially catastrophic consequences are the underlying drivers of dread (Slovic, 2016). The link to cyberspace becomes clear in light of this focus on uncertainty and risk perception since increased dependence on cyberspace elevates people's exposure to potential threats (Brantly, 2021; Hansen & Nissenbaum, 2009). Furthermore, there is high uncertainty surrounding the potential consequences of cybersecurity incidents in the public's eyes (McDermott, 2019). Gomez and Villar (2018) and Kostyuk and Wayne (2021) found a clear disparity between objective assessments of risk and the dread that it creates in cyberspace – a fact that they explained by the public's lack of technological knowledge, which contributes to the high degree of uncertainty surrounding cyberspace.

### Anxiety

Feelings of anxiety are driven by uncertainty and lack of control, which increases risk-aversion and heightens support for risk-minimizing actions (Lerner & Keltner, 2001). We differentiate dread from anxiety, with the former functioning as an anticipatory emotion about a concrete and impending risk, while the latter is a more transitory state of mental uneasiness (Gomez & Whyte, 2020; Huddy et al., 2005). While an initial series of studies found that public exposure to major cyber-attacks can trigger visceral anxiety (Cheung-Blunden et al., 2019; Gross, Canetti, & Vashdi, 2016), subsequent research failed to find a link between the onset of anxiety and political outcomes (Shandler et al., 2022; Backhaus, Gross, Waismel-Manor, Cohen,



& Canetti, 2020). Empirical research focusing on exposure to traditional violence (Haidt, 2003) and cyber-violence (Shandler et al., 2022) have both concluded that anxiety does not translate to concrete shifts in political attitudes. When applied to trust outcomes, the transitory vagueness of anxiety, being a general state of uneasiness, means that it is not always clear whether latching oneself to leaders will dispel the negative feeling. As such, we expect that this feeling will not intervene in our research model.

Based on this literature, we propose the following hypotheses relating to the mediating role of emotions in driving political effects following exposure to degradative cyber-attacks. The hypothesized mechanism is visualized in Figure 1.

**Hypothesis 2:** *Exposure to cyber-attacks will cause heightened anger which will, in turn, increase confidence in the government's ability to protect against future attacks.*

**Hypothesis 3:** *Exposure to cyber-attacks will cause heightened dread which will, in turn, decrease confidence in the government's ability to protect against future attacks.*

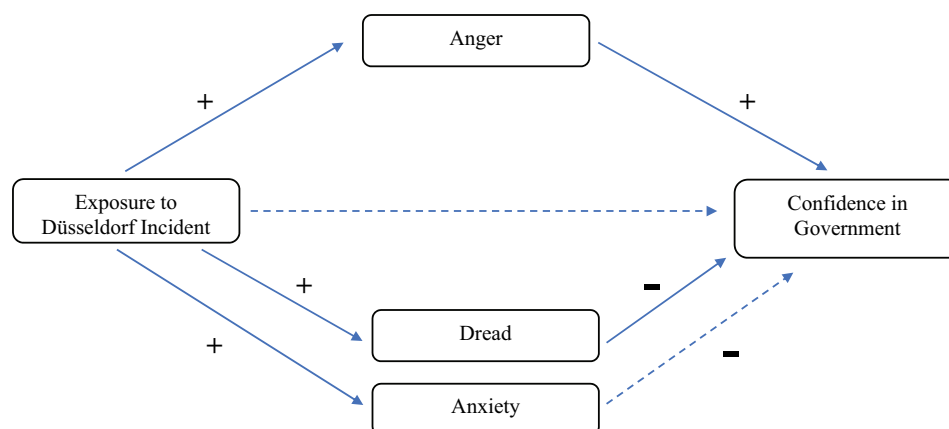
**Hypothesis 4:** *Exposure to cyber-attacks will cause heightened anxiety, yet anxiety will have no subsequent effect on confidence in the government's ability to protect against future attacks.*

### **The incident: a ransomware attack in Düsseldorf**

On the night of September 9, 2020, a ransomware attack infected the systems at the Düsseldorf University Hospital, a large hospital in the south of Düsseldorf. Ransomware is a form of malicious software that locks a device to prevent users from accessing their files, often by encrypting data until a ransom is paid (Richardson & North, 2017). As the attack spread throughout the hospital's computer network, thirty servers were encrypted and made inoperable. Patient data was rendered inaccessible, and much of the Wi-Fi-connected medical equipment became unavailable. The hospital was forced to cease operations for many weeks while they repaired damaged systems.

In the chaos, the hospital had to decide what to do with a 78-year-old patient awaiting a life-saving emergency operation to treat a brain aneurysm (Ralston, 2020). The hospital urgently transferred the patient to the Wuppertal Hospital – some 19 miles (30 km) away. The patient was pronounced dead soon thereafter.

Meanwhile, the hackers demanded a hefty ransom to restore access to the locked computer systems. After police informed the perpetrators that the attack had unintentionally spread to a local hospital, the perpetrators provided a digital key and disappeared (Culafi, 2020). At this point, as is the case with all cyber-attacks, exaggerated and overdramatic reports about lethal cyber-attacks flooded airwaves and newspaper columns.



**Figure 1.** Counteracting mediation model of exposure to cyber-attacks on public confidence in government.

Note: Full lines represent significant effects at  $p < .05$ . Dotted lines reflect non-significant effects at  $p > .05$ . Plus (+) symbols signify a positive effect. For example, anger will increase confidence in government. Minus (-) symbols signify a negative effect. For example, dread will lower confidence in government.

Hyperbolic headlines reported “Cyber Attack Suspected in German Woman’s Death” (Eddy & Perlroth, 2020).<sup>4</sup>

As the investigation continued, German officials concluded that Russian operatives perpetrated the attack due to the language of correspondence with the attackers, and since the DoppelMayer malware that was used has its roots among Russian hackers (Culafi, 2020). The official attribution took place several months after the attack had been resolved. Before this time, speculation abounded, yet the attacker’s identity was not known to the public.

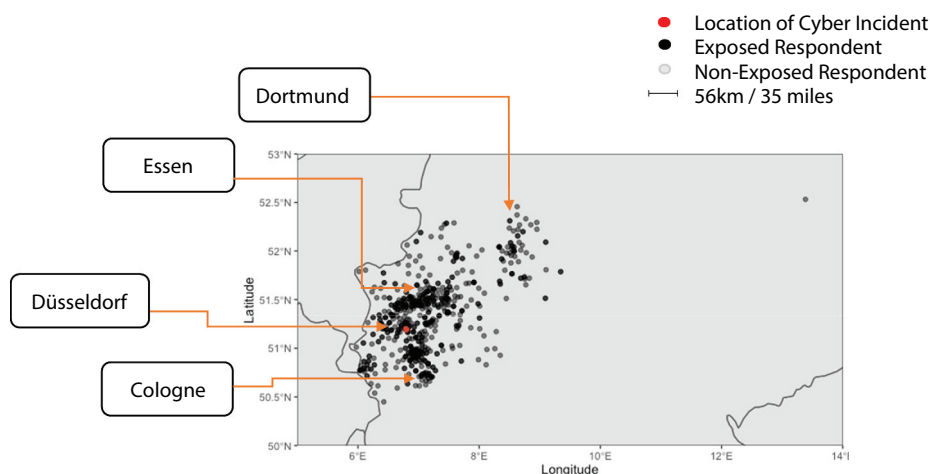
### Methodology

To test our hypotheses, we conducted a survey in the state of North Rhine-Westphalia immediately following the public disclosure of the ransomware attack affecting the Düsseldorf University Hospital. Respondents ( $n = 707$ ) were approached during a seven-day period from 30 September to 6 October 2020 through the Respondi survey company. Media coverage of the incident peaked between September 18–23, and our survey was distributed within one week after this period. The study respondents represented a cross-section of the general population (mean age = 45.4 years,  $SD = 11.09$ ). The sample’s political orientation leans slightly to the left, with 61% of respondents self-identifying as left-leaning, while the gender distribution is 48% female. All respondents are

residents of North Rhine-Westphalia – a state with a population of 18 million. Thirteen percent of all respondents lived in the city of Düsseldorf, with the distance of residence from the attack site ranging from less than one kilometer to 476 km, with a mean of 57 km. We constrained our collection to the state level since too small a zone (i.e., Düsseldorf city center) would have inhibited our ability to measure how diminishing physical proximity influences outcomes, and a zone too wide (i.e., all of Europe) would have encountered a dilemma of participant indifference to far-flung problems. North-Rhine Westphalia strikes a balance between these needs and follows other literature that used state-wide analyses to measure proximity effects to violence (Blanchard et al., 2004; Huddy, Feldman, & Weber, 2007). Respondents’ geographic distribution is depicted in Figure 2, with the location of the Düsseldorf University Hospital marked in red. The figure illustrates that respondents mostly reside in Düsseldorf or other urban centers in the region (e.g., Cologne, Essen)

### Predictor variables (Exposure to the attack)

In designing this study, we were faced with a novel question about what constitutes *exposure* to a cyber-attack. The literature offers varying conceptualizations of exposure such as suffering personal physical harm (Canetti, Elad-Strenger, Lavi, Guy, & Bar-Tal, 2017; Hirsch-Hoefler, Canetti, Rapaport, & Hobfoll, 2016), the act of witnessing



**Figure 2.** Geographical distribution of respondent residency relative to the attack site. Note: Residency is determined based on postal codes submitted by the respondents.

an attack (Bonanno, Galea, Bucciarelli, & Vlahov, 2007), physical proximity to the site of an attack (Besser, Neria, & Haynes, 2009; Bonanno et al., 2007; Huddy & Feldman, 2011), and emotional proximity to an attack (Bonanno et al., 2007). In recent years, an expansive view of what constitutes exposure emerged, including people who view media reports about an attack, since even such indirect exposure is sufficient to cause post-traumatic stress, depression, and anticipatory anxiety (Gadarian, 2010; Williamson, Fay, & Miles-Johnson, 2019).

Applying the question of exposure, for example, to the case of the 9/11 attacks on New York, it would be far too restrictive to claim that only the people in the twin towers were exposed to the attack when all nearby residents who were aware of the incident suffered some form of exposure-related harm. Likewise, research on violent incidents such as the Oklahoma City bombing, the Challenger explosion, and college shootings have demonstrated that nearby persons can suffer physical and emotional consequences from viewing media coverage of the event (Ben-Zur, Gil, & Shamshins, 2012; Gadarian, 2010). Building on this, a recent study by Nussio (2020) credited exposure to a terrorist event in Berlin to all national residents aware of the attack since the mere act of awareness, and regional proximity was sufficient to trigger emotional effects.

As such, we use a broad account of exposure that includes German residents with some degree of physical proximity who are aware of the attack – be it through word of mouth, media coverage, or any other method. This follows the lead of earlier studies that found that awareness of an attack among state residents predicts heightened anxiety and threat perception and leads to distinct political outcomes (Huddy et al., 2007; Skitka, Bauman, & Mullen, 2004). Since our sample is drawn from the state of North Rhine-Westphalia, we measure exposure through the following measure of *awareness*.

**Awareness of the attack.** Awareness is measured by asking respondents to identify which of five possible events occurred in Düsseldorf in the preceding weeks. Options included the ransomware that affected the hospital along with fictitious events such as the mayor resigning following

a corruption scandal, a fire burning down the city library, the city agreeing to let in 5,000 asylum seekers following significant protests, and a final option to indicate that the respondent does not know. 57.7% percent of respondents correctly identified the cyber incident and are designated as the exposed sub-sample.

To add further substance to the discussion of exposure and awareness, we also measure the depth of knowledge of the incident. While the Düsseldorf incident was a significant attack that attracted media attention, it was not at the same level as other international terrorism incidents. Consequently, residents will have varying levels of knowledge about the attack. Therefore, we collect a secondary variable that we label *familiarity*.

**Familiarity with the attack.** Among those respondents who successfully identified the existence of the cyber incident, we followed up with a series of four additional questions to measure the extent of their knowledge about the details of the attack. The questions asked about the location of the hospital where the attack took place, the type of malware used, the identity of the group responsible for the attack, and the method of resolution.

### Outcome variables

**Confidence in government.** Public confidence was measured using a four-item index adapted from Nam (2019) and Van Der Does, Kantorowicz, Kuipers, and Liem (2019). Respondents were asked to indicate the extent to which they feel confident that the German government and security agencies can prevent cyber-attacks, cyber-terrorism, cyber-attacks against critical infrastructure, and lethal cyber-attacks from taking place in the future. All items were rated on a scale of 1 (not at all) to 6 (absolutely). Post-hoc analysis showed the scale to be highly reliable (Cronbach's  $\alpha = 0.932$ ).

### Intervening emotional variables

**Anger.** Anger was measured using the shortened version of the commonly used STAXI measure (State-Trait Anger Expression Inventory; Spielberger, 1988). The scale comprises four items that assess the intensity of anger with the threat of cyber-attacks. Respondents rated items on a scale of



1–6 (1 = not at all; 6 = absolutely). The inventory is scored as the total mean of all items, with higher scores reflecting higher levels of anger (Cronbach's  $\alpha = 0.943$ ).

**Anxiety.** Anxiety was measured via the short form Spielberger state-anxiety inventory-6 (Marteau & Bekker, 1992; Spielberger, 1970). This commonly used six-item index identifies both state and trait forms of anxiety. Respondents were asked to rate on a scale of 1–6 the extent to which their feelings correspond to different items when thinking about the threat of cyber-attacks (1 = not at all; 6 = absolutely). Half of the items represent negative feelings and emotions (e.g., 'I feel upset,' 'I feel worried'), and the other half represents positive feelings and emotions (e.g., 'I feel relaxed,' 'I feel content') (Cronbach's  $\alpha = 0.843$ ).

**Dread.** Dread was measured using a ten-item scale developed by Gomez and Villar (2018) to measure dread in cyberspace. Questions ask respondents the extent to which they perceive different elements of cyberspace as threatening and included items such as: 'Cyberspace is a deceptive environment' and 'I am suspicious of actions and outcomes in and through cyberspace.' All items were rated on a scale of 1–6 (1 = not at all; 6 = absolutely) (Cronbach's  $\alpha = 0.813$ ).

### Covariates

The covariates collected included: age, gender, level of education, family income, employment status, computer literacy (a summative index of four items adapted from Kostyuk & Wayne, 2021), and personal threat perception from terrorism (Gross et al., 2017). The full survey instrument with all questions can be found in Online Appendix G.

## Results

### Analytical strategy

To estimate the effect of exposure to the cyber incident on confidence in government, we would ideally abide by the strict dictates of experimental research with respondents randomly assigned to treatment and control conditions. In our case, we *intentionally departed from the confines of*

*laboratory-controlled conditions with the aim of examining real-world exposure.* The advantage of this method is that our study has higher external validity than controlled experiments that rely on artificial experimental manipulations to simulate exposure. The disadvantage of this method is that we cannot ensure controlled randomization into the experimental conditions. Indeed, balance checks revealed significant differences across treatment and control conditions for age, gender, and income.

To combat this imbalance, we employ the commonly used technique of propensity score matching, which is an effective method for estimating effect sizes in non-experimental settings (Dehejia & Wahba, 2002; Morton & Williams, 2010). The idea behind propensity score matching is to identify comparable participants among the exposed and non-exposed groups that are balanced according to relevant covariates, and to remove outlier subjects from the dataset. We utilize the stricter exact matching technique (rather than the more permissive nearest-neighbor matching approach), which resulted in a reconstructed and balanced dataset with a sample size of 595 (see Walejko et al., 2020 for a strong defense of how exact matching enables the identification of near causal effect in non-experimental studies). In the subsequent results section, we utilize this matched dataset for all analyses, although we show in Online Appendix B that our results hold even for the raw (unmatched) data.

### Preliminary analyses

In terms of our primary independent variable, *awareness*, we find that 54% of respondents were aware of the ransomware incident involving the Dusseldorf University Hospital, compared to 46% of respondents who were oblivious to the incident. Among those respondents with a base level of awareness, we discerned mixed levels of familiarity with the incident's details. 52% of aware respondents demonstrated familiarity with 1–2 pieces of information regarding the event (the hospital's location, the manner of the incident's resolution, etc.), while only 15% exhibited comprehensive familiarity with all details.

Our next step was to verify the emotional effects of incident awareness. This has the benefit of

testing whether this form of exposure causes differential responses among aware and unaware respondents at the most basic level. We find that exposure is associated with significantly higher levels of *anger*, *dread*, and *anxiety*. We tested the significance of these differences by running three independent t-tests, demonstrating that exposure to the incident trigger significantly higher levels of anger ( $t(593) = 4.446$ ,  $p = .000$ ) and dread ( $t(593) = 2.925$ ,  $p = .003$ ), yet no difference in the levels of anxiety ( $t(593) = 1.551$ ,  $p = \text{n.s.}$ )

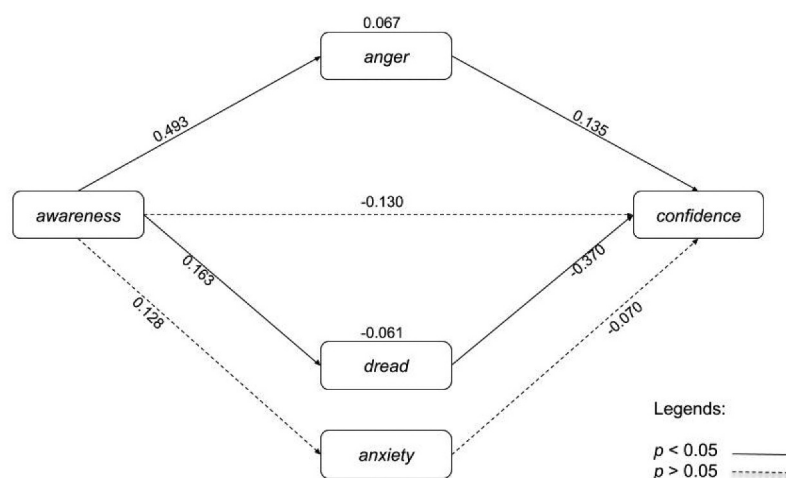
### Main analysis

On the basis of the preliminary analysis, we move to test the hypothesized counteracting mediation mechanism. The results of the mediation analysis appear in Figure 3. As expected, exposure significantly increases both anger ( $\beta = 0.493$ ,  $p = .000$ ) and dread ( $\beta = 0.163$ ,  $p = .003$ ) while there are no statistically significant differences in levels of anxiety. Looking at the B' path, both anger and dread significantly influence confidence levels, though they affect the outcome variable in countervailing directions. A one-unit increase in anger increases the reported level of confidence by 0.135 units. Inversely, a unit increase in dread lowers confidence by 0.370 units. Anxiety, as hypothesized, does not exert influence over the dependent variable.<sup>5</sup> We note the disparity between the

coefficient values of the effect of anger and dread, with dread diminishing confidence at nearly three times the level that anger props it up. Mediation analyses confirms that the effect of awareness on confidence is significantly mediated through both anger ( $\beta = 0.067$ ,  $p = .006$ ) and dread ( $\beta = -0.061$ ,  $p = .024$ ) in countervailing directions.

The countervailing pull of anger and dread is further illustrated in the mediation analysis results in Table 1. The fact that dread pulls down confidence to a greater degree than anger drives it up leads to a significantly negative total effect ( $\beta = -0.200$ , LLCI =  $-0.372$ , ULCI =  $-0.016$ ) and supports our first hypothesis. Our model incorporates several covariates, including computer literacy, political position, exposure to cybercrime, and exposure to COVID-19. Of these, only computer literacy and political position significantly affect confidence.

As a next step, recognizing the still-open question of what constitutes exposure to cybersecurity incidents, we replace the independent variable of *awareness* with *familiarity* to examine whether depth of knowledge is a better proxy for exposure. As described above, all participants who exhibited a base level of familiarity with the attack were asked a series of follow-up questions to explore the level of knowledge regarding the specifics of the incident. As such, we re-specify the above model with *familiarity* serving as the independent variable. The results demonstrate that *familiarity* has no direct



**Figure 3.** Counteracting mediation model of exposure to cyber-attacks on support for retaliation using matched dataset.

Note: Values reflect OLS regression coefficients. Models control for computer literacy, political orientation, past exposure to cybercrime, and covid-exposure.

**Table 1.** Mediation analysis results.

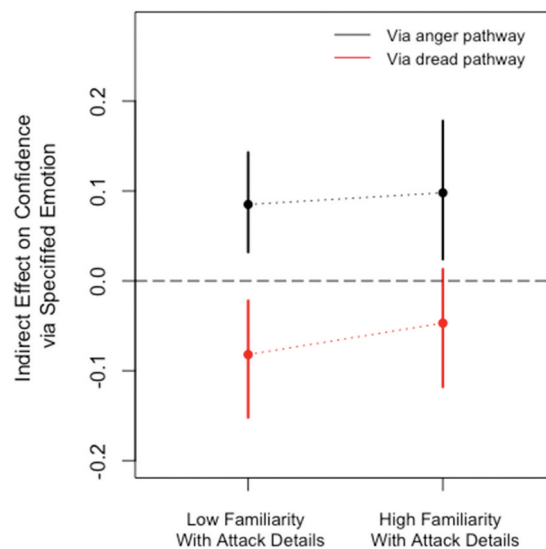
	Outcome variable: Anger (mediator)			Outcome variable: Dread (mediator)			Outcome variable: Confidence (DV)		
	Coeff	z	p	Coeff	z	p	Coeff	z	p
Awareness (IV)	0.493	4.516	0.000	0.163	2.896	0.004	-0.130	-1.509	0.131
Anger (mediator)	---	---	---	---	---	---	0.135	3.351	0.001
Dread (mediator)	---	---	---	---	---	---	-0.370	-4.666	0.000
Anxiety (mediator)	---	---	---	---	---	---	-0.070	-1.147	0.251
Computer Literacy	-0.029	-0.131	0.895	0.057	0.521	0.603	-0.410	-2.518	0.012
Political Position	0.183	1.579	0.114	-0.039	-0.638	0.523	-0.246	-2.753	0.006
Past exposure to Cybercrime	0.208	1.833	0.067	-0.078	-1.407	0.160	-0.002	0.028	0.978
COVID-19	0.008	0.075	0.940	0.028	0.484	0.628	0.018	0.197	0.844
							Coeff	S.E.	
Direct Effect							-0.130	0.086	
Indirect Effect (Anger)							[-0.305, 0.031]	0.024	
Indirect Effect (Dread)							[0.027, 0.125]	0.027	
Total Effect							[-0.126, -0.017]	0.229	
							-0.769	[-1.218, -0.314]	

Note: Demographic variables of age, gender, and income were included in the propensity score matching and were therefore excluded from the regression model.

effect on confidence ( $\beta = 0.212$ ,  $p = \text{n.s.}$ ), nor is there an indirect effect via anger ( $\beta = -0.020$ ,  $p = \text{n.s.}$ ) or dread ( $\beta = 0.073$ ,  $p = \text{n.s.}$ ).

We further test whether familiarity amplifies or minimizes the effect of awareness on confidence, such that learning more details about the attack would either assuage or frighten exposed people to a greater degree. The findings, displayed in Figure 4, reveal that the countervailing mediation mechanism described above holds at low levels of familiarity.

However, something interesting occurs once exposed individuals accrue knowledge about the attack. As can be seen by the fact that the confidence interval for dread dissects the zero-line, people with high levels of familiarity experience significantly less dread. Presumably, having learned more about the attack, the respondents understand that cyber-attacks are limited in scope and do not pose a cataclysmic and immediate threat. As a result of the reduced levels of dread among high-familiarity individuals, we no

**Figure 4.** Indirect treatment effect conditional upon incident familiarity.

Note: Bars represent 95% confidence intervals. Dotted lines are included only to highlight differences in indirect treatment effects at different levels of familiarity.

longer observe such a stark reduction in public confidence. The implication of this finding is that the harmful political effects of exposure can be reduced if exposed individuals attain higher familiarity with the event's details. The full regression results of this familiarity effect appear in Online Appendix C.

As a final step, we ran a series of sensitivity analyses to test whether our countervailing mediation model is robust against potentially confounding pre-treatment covariates – essentially examining if there are conveniently missing variables that would undermine these findings. The findings, reported in Online Appendix D, demonstrate that it would require an unusually large confounder to be omitted to negate the identified mediating effect. Therefore, the effect is robust against alternative explanations.

## Discussion

This study employed a cross-sectional survey design that took advantage of a cyber-attack in Düsseldorf in September 2020. In doing so, this study empirically evaluates how exposure to cyber-attacks on critical infrastructure influences public confidence, and through what psychological mechanism the effect takes place. We expect the results to bear substantial public importance as the increasing frequency of cyber operations leads to growing numbers of people being exposed to cyber incidents. We note several significant findings that emerge from this study.

First, this study makes a theoretical contribution to the public opinion literature. In contrast to the well-documented effect of conventional violence producing short-term increases in public confidence (Chanley, Rudolph, & Rahn, 2000), we find that cyber-attacks *diminish* public confidence in government. If much of the cyber literature questions whether cyber violence abides by the tenets of conventional political theories, we offer a distinctly negative response. We find that cyber-attacks are not just another method of violence interchangeable with bombs, guns, or rockets. Cyber-attacks occur in a fundamentally different domain with unique qualities that alter traditional political outcomes. While our empirical design cannot causally tie the observed political effect to any particular quality of cyberspace, our findings are

complemented by past research that show how the absence of clear attribution in cyberspace (Egloff, 2020), the lack of domain expertise amongst the public (Kostyuk & Wayne, 2021), and the dread associated with cyberspace (Gomez & Villar, 2018) combine to produce new political effects. In practical terms, *we find that governments cannot rely on a unifying social-cohesion effect following cyber-attacks* since the public is liable to perceive the authorities as incapable of defending against future attacks.

This finding suggests that intensifying cyber-attacks can cause severe social damage. Much of the attention following cyber-attacks focuses on concrete damage to infrastructure, financial consequences, and invasions of privacy. While all of these are important, we suggest that the focus on physical consequences obscure a more insidious effect – *undermining public confidence in government*. This confidence effect can trigger a downward spiral since effective cybersecurity requires close cooperation between end-users, cybersecurity vendors, and government agencies. If the public does not trust that the government can effectively guard against damaging cyber-attacks against public institutions, this will amplify a sense of fatalism in cyberspace where seemingly omniscient and malicious perpetrators run havoc. We note that a distinction can be made between actions that explicitly seek to undermine public confidence and social cohesion (i.e., misinformation operations), and actions where the primary aim is something else (data manipulation, physical destruction, etc.). In the case of the former, any diminution of public confidence is a direct objective of the action, and the effect is not contingent upon emotional reactivity to an action (Gomez, 2020). This is in large part why we limit our analysis to degradative attacks. For these attacks, the focus of the authorities will typically be on the immediate first order effects, yet our findings encourage them to carefully consider how the attack could impact public confidence as a second-order consequence.

Second, we find a theoretically divergent pattern in the emotions and public opinion literature. In the aftermath of conventional political violence, research notes that anxiety and anger are two prominent emotions that explain subsequent political effects (Huddy, Feldman & Cassesse, 2007).

However, a series of cyber studies have consistently found that anxiety is less germane in the aftermath of cyber violence (Shandler et al., 2022; Backhaus et al., 2020). Our study corroborates that anxiety is not a predominant emotion experienced by people exposed to significant cyber-attacks. Instead, we verify that dread is a more relevant emotion. Our counteracting mediation model demonstrates that experiencing anger amplifies trust in government following cyber-attacks, while dread minimizes the political effects. This finding suggests that governments may want to fan the flames of public anger rather than letting dread proliferate to avoid diminished public confidence in the aftermath of cyber-attacks.

A third implication of these results is that they clarify what constitutes ‘exposure’ to cyber incidents. Our findings reveal that *awareness of an attack* combined with *geographical proximity* to the attack site is sufficient to activate the various emotional and political effects discussed. However, this effect can be mitigated by increased *familiarity* or depth of knowledge of the attack, which lowers the feeling of dread. This finding accords with previous studies that demonstrate the importance of knowledge in shaping perceptions and preferences in cyberspace (Gomez & Whyte, 2021). On a practical level, the ability of knowledge to mitigate negative outcomes offers valuable insights for public officials who seek to minimize panic by limiting information flow. We show that once the media begin reporting on an attack, it is in the interest of leaders to increase the flow of information, since understanding the limited scope of a cyber-attack minimizes the dread-inducing sensation that otherwise occurs.

Fourth, our results make a methodological contribution by reinforcing the added value of ecologically valid experimental techniques in advancing this nascent research agenda. There is a noted paucity of externally valid research in the study of cybersecurity (Spring et al., 2017). In some ways, this is understandable since cyber-attacks often occur under a shroud of secrecy, making it challenging to acquire valuable real-time data on the effects. However, this difficulty does not curtail the importance of complementing the early controlled research in the field with more externally valid real-world studies.

Though it lies beyond the remit of this paper, our findings highlight a promising research direction relating to cyber escalation. An evolving line of research has accentuated how public enthusiasm for the use of cyber-power may encourage the onset of military escalation since, for example, governments need not worry about public criticism following military casualties (Kreps & Schneider, 2019; Shandler, Gross, & Canetti, 2021). In contrast to this view, our findings suggest that public exposure to cyber-attacks may inhibit public support for escalation due to the dread response that reduces trust in the government’s ability to defend its citizens.

In anticipation of future research refining the political effects of public exposure to cyber threats, we point to several key lessons and limitations that emerge from this study. The psycho-political effects of cyber-attacks are intricately wrapped up in the hyperbolic media reporting that surrounds the incidents. To the extent that the Düsseldorf attack was depicted as a first-of-a-kind attack, the results may not readily generalize to other cyber-attacks. Since the public is already primed to believe that cyber-attacks are a deadly phenomenon, we do not expect the first-of-a-kind narrative to have distorted the observed effects. Nevertheless, research should always account for the tone and nature of media reporting.

Furthermore, the geographical proximity effect in our study was limited to a state-level unit of analysis. Future studies would do well to specify the geographical diffusion of the effects of cyber-attacks to a more exact degree and encompass a wider area. Likewise, it would be interesting to ponder if and how the implications of our study might extend to non-democratic regimes. Emerging research suggests that autocratic regimes too need be sensitive to public opinion on security matters (Quek & Johnston, 2017). On the surface, autocratic countries have greater control over the information environment than their democratic counterparts, with a consequence being that the public is less likely to be exposed to reporting about security incidents. Yet digging a bit deeper, we see that even in non-democratic countries that strictly regulate traditional and digital media, Internet users have demonstrated an ability to access and disseminate information (Roberts, 2020). When information trickles out about a censored security incident, the act of censorship can further *amplify* public dread,



since people feel even more uncertain and unsure of their level of vulnerability. According to this view, we would expect to see countervailing effects – the absence of media reporting would mitigate any confidence effects, while the dissemination of unverified rumors would amplify the effects.

The public is facing a rising tide of cyber-attacks that are likely to increase over time. Even as the risk of physically catastrophic cyber-attacks diminishes, cyber-attacks can still levy enormous harm by undermining trust in government and triggering insidious political outcomes. In this paper, we sought to empirically verify this phenomenon by testing how a ransomware attack in Düsseldorf altered public confidence. Our results affirm that contrary to classical theories of conventional violence, exposure to cyber-attacks decreases confidence in government. As attacks proliferate, the cumulative effects could realign public trust and expectations regarding the government's ability to protect their citizenry from a new generation of cyber threats. We also offer a new counteracting double-mediation model that illustrates the emotional mechanism underpinning shifts in confidence. This model emphasizes the importance of reevaluating political psychology theories for a cyber age.

## Notes

1. Of which Düsseldorf is the state capital.
2. We interpret public institutions broadly as being entities that serve some public purpose – healthcare, energy, transportation, communication, banking and finance, and more. Public institutions will often overlap with critical infrastructure, yet we refrain from using that term since different countries incorporate different industries under the heading of critical infrastructure.
3. Following best practice, we use the phrase public confidence interchangeably with 'trust in government', 'political confidence', and 'political trust' (see Citrin & Stoker, 2018).
4. In the forensic analyses of the incident, the death was found to be a second order effect of the cyber-attack, and not a direct cause. Yet for the weeks after the attack was first reported, and during the period of the survey, the grandiose reporting about lethal cyber-attacks continued.
5. Both the emotion variables and the outcome variable were measured on a six-point scale. When replacing the variables with standardized coefficients, anger exerts an effect of 0.173 units, and dread exerts an effect of -0.236 units. These standardized figures suggest a medium to large effect magnitude.

## Acknowledgments

We are grateful to Steffi Bernhuber, Lea Schaad, and Bianca Villar for their assistance in fielding and translating our survey. This article benefited greatly from the feedback offered at a 2021 colloquium hosted by Myriam Dunn Cavelty at the ETH Zurich Center for Security Studies, a presentation at Daphna Canetti's Political Psychology Lab at the University of Haifa, a session of the Digital Issues Discussion Group led by Nadiya Kostyuk and Christopher Whyte, and a panel at the 2021 annual conference of the International Society of Political Psychology. We appreciate the generous input of the article reviewers.

## Data availability statement

Data, analysis files and appendices are available at: [https://osf.io/v7fex/?view\\_only=b07970a1df30449c9f4404ecb2f9a5f3](https://osf.io/v7fex/?view_only=b07970a1df30449c9f4404ecb2f9a5f3)

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

The author(s) reported there is no funding associated with the work featured in this article.

## Notes on contributors

**Miguel Alberto Gomez** is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich. He holds a Masters degree in International Security from the *Institut Barcelona d'Estudis Internacionals* and is currently completing his doctoral studies externally at the *Universität Hildesheim*. He was a lecturer at both the De La Salle University and the College of St. Benilde in the Philippines and has worked in the information security industry before joining academia. His area of research is centered around cybersecurity. Specifically, he is interested in the strategic use of cyberspace as an instrument of national power and the cognitive and affective factors that influence decision-making in this domain.

**Ryan Shandler** is a postdoctoral fellow at the Blavatnik School of Government, University of Oxford, and a postdoctoral research fellow at Nuffield College. Ryan's research interests lie at the intersection of international security and political psychology, where he explores how emerging technologies elevate the role of public opinion in international affairs. Methodologically, Ryan conducts experiments that expose participants to cyber threats in order to measure the long-term societal, political, and psychological consequences.

## ORCID

Ryan Shandler  <http://orcid.org/0000-0002-0931-2014>  
 Miguel Alberto Gomez  <http://orcid.org/0000-0001-8575-2188>

## References

- 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. doi:10.1089/cyber.2019.0692
- Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks In Benson, V., & Mcalaney, J (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press.
- Baldwin, T. E., Ramaprasad, A., & Samsa, M. E. (2008). Understanding public confidence in government to prevent terrorist attacks. *Journal of Homeland Security and Emergency Management*, 5(1). doi:10.2202/1547-7355.1319
- Ben-Zur, H., Gil, S., & Shamshins, Y. (2012). The relationship between exposure to terror through the media, coping strategies and resources, and distress and secondary traumatization. *International Journal of Stress Management*, 19(2), 132–150. doi:10.1037/a0027864
- Besser, A., Neria, Y., & Haynes, M. (2009). Adult attachment, perceived stress, and PTSD among civilians continuously exposed to terrorism in southern Israel. *Personality and Individual Differences*, 47(8), 851–857. doi:10.1016/j.paid.2009.07.003
- Blanchard, E. B., Kuhn, E., Rowell, D. L., Hickling, E. J., Wittrock, D., Rogers, R. L., & Steckler, D. C. (2004). Studies of the vicarious traumatization of college students by the September 11th attacks: Effects of proximity, exposure and connectedness. *Behaviour Research and Therapy*, 42(2), 191–205. doi:10.1016/S0005-7967(03)00118-9
- Bleich, A., Gelkopf, M., & Solomon, Z. (2003). Exposure to terrorism, stress-related mental health symptoms, and coping behaviors among a nationally representative sample in Israel. *Jama*, 290(5), 612–620. doi:10.1001/jama.290.5.612
- Bonanno, G. A., Galea, S., Bucciarelli, A., & Vlahov, D. (2007). What predicts psychological resilience after disaster? The role of demographics, resources, and life stress. *Journal of Consulting and Clinical Psychology*, 75(5), 671. doi:10.1037/0022-006X.75.5.671
- Bonanno, G. A., & Jost, J. T. (2006). Conservative shift among high-exposure survivors of the September 11th terrorist attacks. *Basic and Applied Social Psychology*, 28(4), 311–323. doi:10.1207/s15324834basp2804\_4
- Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, 7(1), tyab001. doi:10.1093/cybsec/tyab001
- Canetti, D. (2017). Emotional distress, conflict ideology, and radicalization. *P.S: Political Science & Politics*, 50(4), 940–943.
- Canetti, D., Elad-Strenger, J., Lavi, I., Guy, D., & Bar-Tal, D. (2017). Exposure to violence, ethos of conflict, and support for compromise: Surveys in Israel, East Jerusalem, West Bank, and Gaza. *Journal of Conflict Resolution*, 61(1), 84–113. doi:10.1177/0022002715569771
- Canetti, D., Rapaport, C., Wayne, C., Hall, B., & Hobfoll, S. (2013). An exposure effect? Evidence from a rigorous study on the psycho-political outcomes of terrorism. In Sinclair, S. J., & Antonius, D (Eds.), *The Political Psychology of Terrorism Fears*. (New York, NY: Oxford University Press), 193–212.
- Chanley, V. A., Rudolph, T. J., & Rahn, W. M. (2000). The origins and consequences of public trust in government: A time series analysis. *Public Opinion Quarterly*, 64(3), 239–256. doi:10.1086/317987
- Cheung-Blunden, V., Cropper, K., Panis, A., & Davis, K. (2019). Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion*, 19(8), 1353. doi:10.1037/emo0000508
- Citrin, J., & Stoker, L. (2018). Political trust in a cynical age. *Annual Review of Political Science*, 21(1), 49–70. doi:10.1146/annurev-polisci-050316-092550
- Culafi, A. (2020). Potential ransomware-related death still under investigation. *Search Security*. CRC Press. 1 October 2020.
- de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7. doi:10.1016/j.giq.2017.02.007
- Dehejia, R. H., & Wahba, S. (2002). Propensity score-matching methods for nonexperimental causal studies. *Review of Economics and Statistics*, 84(1), 151–161. doi:10.1162/003465302317331982
- Dinesen, P. T., & Jæger, M. M. (2013). The effect of terror on institutional trust: New evidence from the 3/11 Madrid terrorist attack. *Political Psychology*, 34(6), 917–926. doi:10.1111/pops.12025
- Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. 2012 4th International Conference on Cyber Conflict (CYCON June 2012), Tallinn, Estonia, (pp. 1–13). IEEE.
- Dunn Cavelty, M. (2019). The materiality of cyberthreats: Securitization logics in popular visual culture. *Critical Studies on Security*, 7(2), 138–151. doi:10.1080/21624887.2019.1666632
- Eddy, M., & Perlroth, N. (2020). Cyber attack suspected in German woman's death. *New York Times*. 18 September 2020.
- Egloff, F. J. (2019). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, 41(1), 55–81. doi:10.1080/13523260.2019.1677324
- Egloff, F. J. (2020). Public attribution of cyber intrusions. *Journal of Cybersecurity*, 6(1), tyaa012. doi:10.1093/cybsec/tyaa012
- Egloff, F. J., & Wenger, A. (2019). Public attribution of cyber incidents. *CSS Analyses in Security Policy*, 244.

- Fischer, A. H., & Roseman, I. J. (2007). Beat them or ban them: The characteristics and social functions of anger and contempt. *Journal of Personality and Social Psychology*, 93(1), 103. doi:10.1037/0022-3514.93.1.103
- Gadarian, S. K. (2010). The politics of threat: How terrorism news shapes foreign policy attitudes. *The Journal of Politics*, 72(2), 469–483. doi:10.1017/S0022381609990910
- Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, 38(2), 41–73. doi:10.1162/ISEC\_a\_00136
- Gomez, M. A. N. (2019). Sound the alarm! Updating beliefs and degradative cyber operations. *European Journal of International Security*, 4(2), 190–208. doi:10.1017/eis.2019.2
- Gomez, M. A. (2020). Cyber-enabled information warfare and influence operations. In C. Whyte, A. T. Thrall, & B. M. Mazanec (Eds.), *Information warfare in the age of cyber conflict* (pp. 132–146). New York: Routledge.
- Gomez, M. A., & Villar, E. B. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*, 6(2), 61–72. doi:10.17645/pag.v6i2.1279
- Gomez, M. A., & Whyte, C. (2020). Cyber wargaming: Grappling with uncertainty in a complex domain. *Defense Strategy & Assessment Journal*, 10(1), 95–135.
- Gomez M Alberto and Whyte C. (2021). Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. *International Studies Quarterly*, 65(4), 1137–1150. doi:10.1093/isq/sqab034
- Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber-terrorism. *Bulletin of the Atomic Scientists*, 72(5), 284–291. doi:10.1080/00963402.2016.1216502
- 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.
- Haidt, J. (2003). The Moral Emotions. In R. J. Davidson, K. R. Scherer, & H. H. Goldsmith (Eds.), *Series in Affective Science. Handbook of Affective Sciences* (pp. 852–870). Oxford: Oxford University Press.
- Halperin, E., Russell, A. G., Dweck, C. S., & Gross, J. J. (2011). Anger, hatred, and the quest for peace: Anger can be constructive in the absence of hatred. *Journal of Conflict Resolution*, 55(2), 274–291. doi:10.1177/0022002710383670
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53(4), 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x
- Hirsch-Hoefler, S., Canetti, D., Rapaport, C., & Hobfoll, S. E. (2016). Conflict will harden your heart: Exposure to violence, psychological distress, and peace barriers in Israel and Palestine. *British Journal of Political Science*, 46(4), 845–859. doi:10.1017/S0007123414000374
- Huddy, L., & Feldman, S. (2011). Americans respond politically to 9/11: Understanding the impact of the terrorist attacks and their aftermath. *American Psychologist*, 66(6), 455. doi:10.1037/a0024894
- Huddy, L., Feldman, S., & Cassese, E. (2007). On the Distinct Political Effects of Anxiety and Anger. In Neuman, W. R., Marcus, G. E., MacKuen, M., & Crigler, A. N (Eds.), *The Affect Effect: Dynamics of Emotion in Political Thinking and Behavior*, University of Chicago Press, 202–230.
- 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. doi:10.1111/j.1540-5907.2005.00144.x
- Huddy, L., Feldman, S., & Weber, C. (2007). The political consequences of perceived threat and felt insecurity. *The Annals of the American Academy of Political and Social Science*, 614(1), 131–153. doi:10.1177/0002716207305951
- Janoff-Bulman, R. (1992). *Shattered assumptions: Towards a new psychology of Trauma*. New York: Free Press.
- Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*, 2(1), 64–87. doi:10.1017/eis.2016.14
- Kaminska M. (2021). Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity*, 7(1), doi:10.1093/cybsec/tyab008
- Kello L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2), 7–40. doi:10.1162/ISEC\_a\_00138
- Kertzer, J. D., Oppenheimer, H., & Zeitzoff, T. (2021). Do cyberattacks corrode?: Cyberattacks and domestic politics. Working Paper.
- Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, 6(2), ogz077.
- Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*, 5(1), tyz007. doi:10.1093/cybsec/tyz007
- Lawson, S. T. (2019). *Cybersecurity discourse in the United States: Cyber-doom rhetoric and beyond*. Abingdon, Oxon: Routledge.
- Leal M M and Musgrave P. (2022). Hitting back or holding back in cyberspace: Experimental evidence regarding Americans' responses to cyberattacks. *Conflict Management and Peace Science*, 073889422211110 doi:10.1177/07388942221111069
- Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality and Social Psychology*, 81(1), 146–159. doi:10.1037/0022-3514.81.1.146
- Lindsay J R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365–404. doi:10.1080/09636412.2013.816122
- Marteau, T. M., & Bekker, H. (1992). The development of a six-item short-form of the state scale of the Spielberger State–Trait anxiety inventory (STAI). *British Journal of Clinical Psychology*, 31(3), 301–306. doi:10.1111/j.2044-8260.1992.tb00997.x
- Maschmeyer L. (2022). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, 1–25. doi:10.1080/01402390.2022.2104253
- McDermott, R. (2010). Decision making under uncertainty. *Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S.*

- Policy, Washington, DC: National Academies Press, pp. 227–241.
- McDermott, R. (2019). Some emotional considerations in cyber conflict. *Journal of Cyber Policy*, 4(3), 309–325.
- Morton, R. B., & Williams, K. C. (2010). *Experimental political science and the study of causality*. New York, NY: Cambridge University Press.
- Mueller, J. E. (1973). *War, presidents, and public opinion*. New York: Wiley.
- Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, 58, 101122. doi:10.1016/j.techsoc.2019.03.005
- Neria, Y., DiGrande, L., & Adams, B. G. (2011). Posttraumatic stress disorder following the September 11, 2001, terrorist attacks: A review of the literature among highly exposed populations. *American Psychologist*, 66(6), 429. doi:10.1037/a0024791
- Nussio, E. (2020). Attitudinal and emotional consequences of Islamist terrorism. Evidence from the Berlin attack. *Political Psychology*, 41(6), 1151–1171. doi:10.1111/pops.12679
- Quek, K., & Johnston, A. I. (2017). Can China back down? Crisis de-escalation in the shadow of popular opposition. *International Security*, 42(3), 7–36. doi:10.1162/ISEC\_a\_00303
- Ralston, W. (2020). The untold story of a cyberattack, a hospital and a dying woman. *Wired*. November 11, 2020. <https://www.wired.co.uk/article/ransomware-hospital-death-germany>.
- Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10.
- Rid T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32. doi:10.1080/01402390.2011.608939
- Roberts, M. E. (2020). Resilience to online censorship. *Annual Review of Political Science*, 23(1), 401–419. doi:10.1146/annurev-polisci-050718-032837
- Schneider, J. (2021). The cyber apocalypse never came. Here's what we got instead. *Politico*. July 27, 2021. <https://www.politico.com/news/magazine/2021/07/27/cyber-apocalypse-russia-china-warfare-500787>.
- Schneider, J. (2022). A world without trust. *Foreign Policy*. January/February, 2022. <https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust>.
- Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2022). Cyber terrorism and public support for retaliation—a multi-country survey experiment. *British Journal of Political Science*, 52(2), 850–868.
- Shandler, R., Gross, M. L., & Canetti, D. (2021). A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. *Contemporary Security Policy*, 42(2), 135–162. doi:10.1080/13523260.2020.1868836
- Shandler, R., Snider, K., & Canetti, D. (2022). The political psychology of cyberterrorism. In D. Osborne & C. Sibley (Eds.), *The Cambridge handbook of political psychology* (Cambridge handbooks in psychology (pp. 565–581). Cambridge: Cambridge University Press. doi:10.1017/9781108779104.038
- Skitka, L. J., Bauman, C. W., & Mullen, E. (2004). Political tolerance and coming to psychological closure following the September 11, 2001, terrorist attacks: An integrative approach. *Personality and Social Psychology Bulletin*, 30(6), 743–756. doi:10.1177/0146167204263968
- Slovic, P. (2016). *The perception of risk*. New York, NY: Earthscan.
- Snider, K., Zandani, S., Shandler, R., & Canetti, D. (2021). Cyber terrorism, cyber threats and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7(1), tyab019. doi:10.1093/cybsec/tyab019
- Spielberger, C. D. (1970). STAI manual for the State-Trait Anxiety Inventory. *Self-Evaluation Questionnaire*, 1–24.
- Spielberger, C. D. (1988). *Manual for the state-trait anger expression scale (STAXI)*. Odessa, FL: Psychological Assessment Resources.
- Spielberger C D, Reheiser E C and Sydeman S J. (1995). Measuring the Experience, Expression, and Control of Anger. *Issues in Comprehensive Pediatric Nursing*, 18(3), 207–232. doi:10.3109/01460869509087271
- Spring, J. M., Moore, T., & Pym, D. (2017, October). Practicing a science of security: A philosophy of science perspective. Proceedings of the 2017 New Security Paradigms Workshop, Santa Cruz CA USA, (pp. 1–18).
- Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. New York, NY: Oxford University Press.
- Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. USA: Oxford University Press.
- Van Der Does, R., Kantorowicz, J., Kuipers, S., & Liem, M. (2019). Does terrorism dominate citizens' hearts or minds? The relationship between fear of terrorism and trust in government. *Terrorism and Political Violence*, 33(6), 1276–1294.
- Walejko, G., Kriz, B., Bates, N., Bates, N., Bates, N., & Bates, N. (2021). Use of exact matching to examine media's effect on intended behavior the case of the addition of the 2020 census citizenship question. *Public Opinion Quarterly*, 84(4), 1000–1013. doi:10.1093/poq/nfaa057
- Williamson, H., Fay, S., & Miles-Johnson, T. (2019). Fear of terrorism: Media exposure and subjective fear of attack. *Global Crime*, 20(1), 1–25. doi:10.1080/17440572.2019.1569519