THE POLITICAL PSYCHOLOGY OF CYBER-TERRORISM

The Cambridge Handbook of Political Psychology (2021)
Eds. Danny Osborne & Chris G. Sibley.

Ryan Shandler*, Keren LG Snider & Daphna Canetti
University of Haifa, School of Political Science, Israel

Post-Print
(Accepted Manuscript)

* Corresponding Author: ryanshandler@gmail.com

Cite as: Shandler, R., Snider, K.G.L., Canetti, D. (2021). The Political Psychology of Cyber-Terrorism. In D. Osborne & C.G. Sibley (Eds.) *The Cambridge Handbook of Political Psychology*. Cambridge University Press.

The Political Psychology of Cyber-Terrorism

1.1 – The Dawn of Cyber-Terrorism....2
1.2 – A Political-Psychology Approach to Cyber-Terrorism....5
1.3 – The Political Effects of Cyber-Terrorism....9
1.3.1 – Cyber Terrorism and Public Confidence....9
1.3.2 – Cyber-Terrorism and Foreign Policy Attitudes....11
1.4 – Conclusion and Future Directions....13
1.5 – References....16

1.1 – The Dawn of Cyber-Terrorism

In May 2020, Israeli authorities reported that they had successfully repelled a sophisticated cyber attack against critical civilian infrastructure (Heller, 2020). According to the report, Iranian-connected attackers hacked into the country's water systems in an attempt to surreptitiously raise the level of chlorine and kill swathes of civilians. The prospect of catastrophic cyber-terror attacks had long been prophesied, and this report constituted a seminal moment in the development and deployment of tangible cyber strikes against civilians. Yet this attack certainly wasn't the first example of cyber-attacks threatening physical damage. In 2018, the United States Department of Homeland Security reported that Russian cyber operatives had successfully infiltrated the control rooms of power plants across the United States (Sanger, 2018). Some years earlier, in 2015, reports emerged that unknown hackers had struck a steel mill in Germany, causing a blast furnace to malfunction, and resulting in explosive damage (Zetter, 2015). Collectively, these attacks heralded the dawn of kinetic cyber-terrorism – the "credible capability to use cyber attacks to achieve kinetic effects" (Applegate 2013, p. 3).

The phenomenon of cyber-terrorism raises a series of questions for political psychologists, most importantly – is cyber-terrorism a topic worth researching? This question does not belittle the significance of the concept, but rather probes the extent to which cyber-terrorism is a distinct phenomenon with underlying mechanisms that diverge from classical (i.e., physical or kinetic) terrorism. In writing this chapter, we assert an affirmative answer. Cyber-terrorism poses a qualitatively new threat to modern society, and the manner that people perceive and respond to the threat is distinctly different from conventional threats of terrorism and political violence. Public polling supports this contention, with surveys revealing mounting trepidation among the public about the destructive capacity of cyber-terrorism (McCarthy, 2016; Norman, 2018). This perception of the scope of a cyber threat may or may not resemble an objective reality (see for example Lawson, 2019; Lewis, 2017; Valeriano and Maness, 2015), yet

the fact that the public views it as such can have tangible political consequences. In short, the nature of terrorism is shifting - our understandings of the effects of new forms of terrorism need to shift, too. In this chapter, we meet this need by mapping a budding collection of theories and empirical research and proposing a consolidated mechanism according to which we can understand the psycho-political effects of exposure to cyber-terrorism. The essence of our argument can be summarized as follows:

> Exposure to cyber-terrorism causes shifts in political attitudes through intervening mechanisms comprising emotional distress. Both the emotional intervening variables and the political outcomes will bear similarities to those following exposure to conventional terrorism, although the direction and strength of these effects will vary. This variance reflects the unique features of cyberspace including attribution difficulties, ease of entry, transnational reach, and the abundance of digitally-connected targets - and also the significant gap in civilian expertise regarding cyberspace, which results in widespread misperceptions and inflated emotional distress.

How, though, are we to define cyber-terrorism? Dorothy Denning's seminal, yet relatively narrow, understanding of cyber-terrorism as the 'convergence of terrorism and cyberspace' remains the best-known and most widely-used definition (Denning, 2000, p. 71). Yet we prefer the more recent variants that acknowledge that, like with terrorism, cyber-terrorism must produce physically destructive consequences (Denning, 2007; Eggloff, 2020). For example, a widely adopted definition by Lachow (2009, p. 101) views cyber-terrorism as "*a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological*". Yet importantly, Lachow adds an additional 'physically destructive' requirement, noting that "*[t]he attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples… Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [be cyber-terrorism]*" (p.101). Adopting this definition, we distinguish our analysis from cyber crime, cyber vandalism and information warfare – some of which lack the requisite intent to intimidate and coerce the public in pursuit of political goals, and all of which lack the requisite destructive properties to be cyber-terrorism.

Many of the studies reviewed throughout this chapter specifically differentiate *lethal cyber-terrorism* from *non-lethal cyber-terrorism.* Lethal cyber-terrorism refers to cyber terror attacks that cause lethal consequences as a first- or second- degree outcome of the attack. For example, a cyber terror attack that causes a train to derail would be considered lethal cyber-terrorism. So too would the September 2020 cyber attack against a Dusseldorf hospital that caused a patient's death after the hospital systems went offline (Tidy, 2020).[1] These kinds of attacks are exceedingly rare and reflect a future-oriented view of what cyber-terrorism could be. While scholars have rightly stepped back from an earlier and premature view that envisioned the onset of cyber-Armageddon, this destructive / non-destructive dichotomy of cyber-terrorism is

[1] The designation of this incident as cyber-terrorism is subject to the motivation and identity of the attacker – which are still unknown at the time of publication.

still prevalent in the literature. Non-lethal cyber-terrorism, by contrast, is taken to mean cyber-terror attacks that do not result in lethal consequences. For example, cyber attacks that steal money with the aim of undermining faith in the financial system would be considered non-lethal cyber-terrorism.

An additional dilemma in the definitional debate is whether states may be deemed capable of conducting cyber terrorism. The literature is unsettled on this point. While classical typologies of terrorism often require the involvement of non-state actors – "[t]here exists considerable 'expert' support for the validity of the proposition that states can indeed engage in cyberterrorism" (Macdonald, Jarvis and Nouri, 2015: 62). This is particularly significant, since at this point time, the technical and financial challenges of designing physically destructive cyber weaponry require the resources and technical expertise of states.

Positing the existence of a distinct cyber-terrorism effect that requires the development of new models is a bold claim. Not every technological breakthrough or novel terror strategy warrants the reevaluation of psycho-political theories of exposure, which have proven resilient to change. Cyber-terrorism tracks a middle ground between technological breakthroughs that constitute tactical developments to which traditional political psychology theories still apply, and new strategic weapons such as nuclear power that so fundamentally altered the nature of the terror threat that it required the development of new theories of escalation, deterrence and civilian exposure (Nye, 2011). What makes cyber-terrorism so different from conventional terrorism are several features unique to cyberspace. The ability of perpetrators to act anonymously, or at least impede attempts at attribution, allows actors to avoid detection in a new manner (Lindsay, 2015). The low barriers to entry enable even under-resourced groups who may otherwise be unable to facilitate attacks to attain destructive capacities that don't require financial or infrastructural resources (Eun and Aßmann, 2016).[2] The borderless nature of cyberspace allows actors to project power globally and instantaneously such that its effects are not geographically constrained. And the ubiquitous presence of cyber-outlets enables new avenues to attack both critical infrastructure and civilians in the safety of their own homes.

We note that cyber-terrorism has given rise to a broad range of research topics related to political attitudes, human security, and the behavior and motivations of cyber terror perpetrators. For most of these issues, we are only beginning to see the first trickle of empirical research to buttress the much more prevalent theoretical conjecture. In an attempt to move the field beyond its initial theoretical base, this chapter will focus on the leading empirical studies that have emerged in recent years – studies that primarily concentrate on civilian exposure to cyber-terrorism. We will begin by presenting a consolidated political psychology model of exposure to cyber-terrorism that will guide our analysis throughout the remainder of the chapter. We will then apply this model to two political outcomes that recur in the empirical literature - public confidence and trust in institutions, and foreign policy attitudes (see also Chapter 18). Finally, we will pinpoint the key gaps in our understanding of the psycho-political effects of cyber-

[2] We note a prominent critique of the conventional wisdom that low barriers to entry truly exist in cyberspace (Cavelty, 2010; Denning, 2009; Slayton, 2017). According to this critique, organizations attempting to project cyber force will encounter significant technical and financial challenges since custom-built software requires high level information technology, skills, and substantial financial and organizational resources that are not easily acquired.

terrorism exposure and propose a research agenda that attempts to account for the evolving nature of the field.

1.2 – A Political-Psychology Approach to Cyber-Terrorism

To understand the political effects of exposure to cyber-terrorism, we need to know something about both political systems and human psychology. This dual focus is premised on the idea that people respond to threats in different ways, and only by understanding individual psychological dispositions can we make sense of how exposure translates to concrete political outcomes. A psycho-political approach is especially applicable for cyber-terrorism, since the effects of terror attacks are designed to spark fear and uncertainty in the civilian population. The internal logic of cyber-terrorism views the emotional public as the soft underbelly of society through which terrorists can realize wider political objectives. In practical terms, when the public response to a cyber-terror incident is dominated by feelings of fear or anxiety, public support should increase for protective policies that would lower their perception of the threat (e.g., strengthened cybersecurity regulations). By contrast, public sentiment characterized by anger would likely lead to demands for aggressive and vengeful counter-terrorism responses. Yet reality is rarely so neatly ordered, and we must account for a sophisticated web of conflicting cognitive and affective intervening variables that combine to guide political attitudes and preferences. It is for this reason that we choose to examine cyber-terrorism through the lens of political psychology.

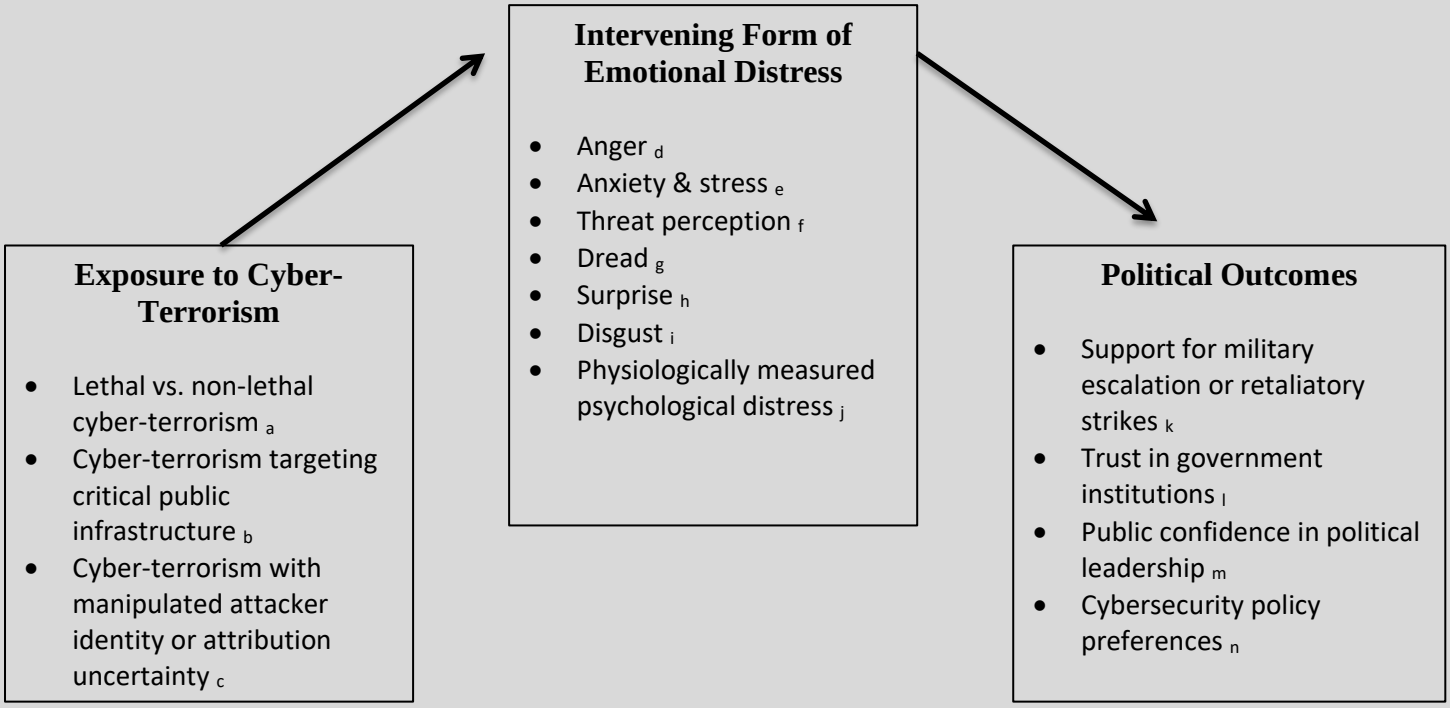
Over the last twenty years, especially since the 9/11 attacks, a political psychology approach has enriched our understanding of the political effects of individual-level exposure to conventional (non-cyber) terrorism and political violence. What we have learned, in essence, is that emotional responses to violence are residues of exposure to life events and external shocks which elicit certain coping behaviors (Canetti, 2017). Arousing specific emotions – even those with similarly negative valence (like anger, anxiety and dread) – causes distinct and often divergent effects on attitudes, behavior and decision making (see Chapter 5). Following from the widespread adoption of these principles, it is now well established that emotional distress explains how exposure to terrorism undermines one's sense of security and feelings of vulnerability (Huddy et al., 2005; Neria et al., 2011; Silver et al., 2002), fosters a threatening worldview and increases support for hardline policies (Bleich, 2003; Bonanno, 2006), causes a rightward shift on security and privacy issues (Janoff-Bulman, 2009) and leads to increased demands for governments to take strong military action against terror groups (Canetti et al., 2013; McDermott, 2010).

Yet how does this literature on conventional terrorism and political violence translate to cyber-terrorism specifically? Scholars have identified several qualities unique to cyber-terrorism that activate distinct emotional responses that influence the strength and direction of political outcomes. Gomez and Villar (2018) and Kostyuk and Wayne (2020) persuasively explain how the public's *lack of technical sophistication and unfamiliarity* in dealing with cyberspace ferment feelings of dread, uncertainty and heightened threat perception. Bada and Nurse (2018) liken this

phenomenon to 'learned helplessness' – a process that fosters apathy since people feel they can neither understand nor defend against cyber attacks. Similarly, a collection of research has highlighted how the inherent *anonymity and mystique* of cyberspace influences psychological responses, with invisible and uncontrollable perpetrators viewed as omniscient digital actors (Dunn Cavelty, 2012; Hansen and Nissenbaum, 2009). McDermott (2019) submits that the *speed of the Internet* and the ensuing need for instantaneous decision making in the context of cyber conflict could increase stress, lower concentration and compromise decision-making. Still another quality of cyber-terrorism that may influence emotional corollaries is its unique depiction in popular media. There is widespread agreement that the *media portrayal of cyber-terrorism as an existential threat*, or in other words, the 'cyber-doom narrative', amplifies threat perception and emotional response to a large degree (Dunn Cavelty, 2019; Jarvis, Macdonald and Whiting, 2017; Lawson, 2019).

Taking these features of cyber-terrorism into account, the literature has begun to coalesce around several key intervening psychological variables that mediate between exposure to cyber-terrorism and political outcomes. These factors appear in Figure 1.

Figure 1. Political Psychology Model of Exposure to Cyber-Terrorism



[a] –Backhaus et al., 2020; Gross, Canetti and Vashdi, 2016, 2017; Shandler et al., 2020; Snider et al., 2020.
[b] - Gomez and Whyte, 2020a; Matzkin, Gross and Canetti, 2020; Gross, Canetti and Vashdi, 2017; Shandler et al., 2020.
[c] - Gross, Canetti and Vashdi, 2016; Jardine and Porter, 2020.
[d] - Matzkin, Gross and Canetti, 2020; Shandler et al., 2020; Wayne, 2019.
[e] - Backhaus et al., 2020; Cheung-Blunden and Ju, 2016; Gomez and Whyte, 2020a; Hua, Chen and Luo, 2018; Jarvis, Macdonald and Whiting, 2017; Matzkin, Gross and Canetti, 2020; Shandler et al., 2020.
[f] – Gomez and Villar, 2018; Kostyuk and Wayne, 2020; Snider et al., 2020.
[g] – Gomez and Villar, 2018; Kostyuk and Wayne, 2020; van Schaik et al., 2017.
[h] – McDermott, 2019.
[i] – McDermott, 2019.
[j] - Backhaus et al., 2020; Canetti et al., 2017.
[k] - Gross, Canetti and Vashdi, 2017; Kreps and Schneider, 2019; Shandler et al., 2020; Shandler, Gross and Canetti, 2020.
[l] - Matzkin, Gross and Canetti, 2020;
[m] - Gross, Canetti and Vashdi, 2017; Kertzer, Oppenheimer and Zeitzoff, 2020; Matzkin, Gross and Canetti, 2020.
[n] – Cheung-Blunden et al., 2019; Kostyuk and Wayne, 2020; Snider et al., 2020.

It's worth noting that the two interceding emotional variables that most frequently appear in cyber-terrorism research are anxiety and anger. These two emotions form a prominent dualism in the literature on political violence—a fact that has converted smoothly into cyber-terrorism research. The political effects of anger and anxiety are grounded in Lerner and Keltner's (2001) emotional appraisal model (see also Chapter 5). According to this theory, anxiety is linked to a sense of uncertainty and lack of control, which increases risk aversion and heightens support for low risk-actions. By contrast, anger arises from a desire to rectify perceived injustice and is therefore associated with more aggressive policy outcomes.

So far, the empirical research has produced consistent outcomes with regards to anxiety. Anxiety is a future-oriented emotional state characterized by feelings of apprehension and accompanied by the arousal of the autonomic nervous system. Following Huddy et al. (2005), we

refer to anxiety as an umbrella term for fear, anxiety and worry. Anxiety is a product of monitoring for potential threats - the more uncertain the threat, the greater the anxiety. As such, exposure to terrorism elicits anxiety because acts of terrorism are perceived as unpredictable, random, and difficult to counter or avoid (Canetti et al., 2009; Slone and Shoshani, 2006). In a series of studies testing whether exposure to cyber-terrorism raises anxiety, Gross et al. (2016) confirmed that both lethal and non-lethal cyber-terrorism are indeed capable of triggering visceral anxiety. This result was replicated by Backhaus et al. (2020), who measured anxiety via salivary cortisol. Cheung-Blunden et al. (2019) has repeatedly identified the onset of anxiety following cyber attacks, with Cheung-Blunden and Ju (2016) replicating this finding under both naturally and experimentally induced anxiety conditions. We note, however, that Gomez and Whyte (2020a) argue that this effect may diminish over time due to the oversaturation of cyber-doom appeals that numb the public. This corresponds with similar findings regarding conventional terrorism, wherein overexposure to terror threats and fearmongering can minimize the salience of the threat.

Anger, too, has featured prominently in the empirical research on cyber-terrorism. Exposure to terror events is understandably accompanied by anger, of which the underlying drive is often defined as a desire to correct perceived injustice (Fischer and Roseman, 2007; Halperin et al., 2011). Since cyber-terrorism directly transgresses norms regarding the use of force, exposure is especially likely to evoke anger and a desire for remedial or retaliatory actions (Gomez, 2020). Recent research suggests that the "dominant response of civilian populations to terror threat is not fear and a desire to reduce future personal risk, but rather anger and a desire for vengeance" (Wayne 2019, p. 5). This finding was buttressed by Shandler et al. (2020) whose multi-country study found that only anger – and not anxiety or threat perception – mediated the relationship between exposure to cyber-terrorism and support for militant policies.

While anger and anxiety have naturally comprised the main focus of the psychological mechanisms underlying exposure to cyber-terrorism, several innovative studies have incorporated alternative emotional and cognitive variables that relate more directly to the particular qualities of cyberspace. Snider et al. (2020) concluded that *threat perception*, a cognitive discernment of threat posed to physical or symbolic resources, plays an important role in mediating exposure to cyber-terrorism and support for cybersecurity policy preferences. Since the scope of the perceived threat is driven by the level of familiarity, we would certainly expect that cyber-terrorism would increase threat perception considering its unfamiliar, unpredictable, and indiscriminate nature. Gomez and Villar (2018) have tied the perception of cyber threats to the feeling of *dread* using the lens of cognitive heuristics, while van Schaik et al. (2017) has also linked cyber threat perception and dread. McDermott (2019) has theorized that surprise and disgust are both variables of interest in the realm of cyber conflict. Since cyber attacks are characterized by a great deal of uncertainty and time urgency, the feeling of *surprise* is likely to shape the nature of decision making and increase the assessment of responsibility (McDermott, 2019). *Disgust*, according to McDermott, would be activated in situations where cyber attacks target critical domestic systems and are linked to demands for aggressive retaliatory responses. Bada and Nurse (2018) and Nurse (2018) have also suggested a role for *apathy* and *shame*.

1.3 – The Political Effects of Cyber-Terrorism

The spectrum of political outcomes associated with exposure to cyber-terrorism is practically boundless. Looking back to conventional terrorism as a guiding force, scholars have examined political outcomes ranging from political ideology and political participation, to radicalization and support for violence. While many of these studies are valuable, it has been noted that many cybersecurity studies tend to lack methodological rigor and epistemological outlooks, falling into the trap of engaging in purely speculative conjecture with low empirical validity (Valeriano and Gomez, 2020). In this chapter, we choose to focus on two political outcomes that have attracted the most empirical research attention - public confidence and foreign policy attitudes.

We highlight these political phenomena for several reasons. Public confidence is a classic variable in the field of political psychology with a deep well of theories and models from which to draw. It is especially fitting to look at public confidence in the context of cyber-terrorism since the twisted logic of terrorism is predicated on provoking a sense of fear and vulnerability in the wider population and undermining confidence in the government. The second political outcome is foreign policy attitudes in general, with a particular focus on support for military retaliation. We examine this topic due to its prominence in the nascent empirical literature on cyber-terrorism. Additionally, this topic raises an interesting question about how cyber terrorism, conducted through a non-physical digital realm, can manifest cross-domain political consequences through heightened militancy and support for real-world military action.

1.3.1 – Cyber Terrorism and Public Confidence

Terrorist attacks are by their very nature designed to erode public confidence and elicit shifts in individual behavior that disrupt daily life. These attacks are designed to shake society's trust in the government's ability to function and defend against future attacks. We define public confidence as the subjective assessment of the ability of governments, leaders and security institutions to prevent attacks and maintain a functioning state (Baldwin, Ramaprasad and Samsa, 2008). Political psychologists have probed this connection at length and produced sophisticated cognitive and affective models that explain how exposure to terrorism translates to heightened or reduced public confidence. Perhaps counter-intuitively, the majority of studies conclude that exposure to terrorism amplifies public support for government policies and public confidence in government institutions (Chanley, 2002; Huddy et al., 2005), a fact that is not necessarily tied to rational processing of the government's competence in the face of the terror threat, but rather by the need for psychological security due to an environment of fear, uncertainty, anger and outrage (see Merolla and Zechmeister, 2009; Sunstein, 2009).

We posit that the advent of cyber-terrorism upends, and even reverses, these mechanisms. The reason for this is that cyber-terrorism possesses qualities that are prone to specifically affect

confidence. Foremost among these is the attribution dilemma, or the quality of ambiguity surrounding the identification of cyber perpetrators. This attributional difficulty works in multiple directions. The absence of knowledge about the identity of an attacker can heighten the perception of risk due to the omniscience so often associated with cyber operatives (Dunn Cavelty, 2012). Alternatively, the lack of attribution could leave victims perplexed rather than terrorized (Gartzke, 2013). A second quality relates to perceptions about the government's ability to identify the perpetrators. If civilians believe that security forces can't or won't identify major cyber attacks, then this acts as a key point of difference in the confidence equation (see Maschmeyer, Deibert and Lindsay for an analysis of how threat reporting underrepresents particular segments of society). Though it is closely related, we must pause and distinguish between information warfare and cyber-terrorism. The majority of the literature relating to cyber threats and public confidence relates to disinformation campaigns against democratic institutions using cyber tools. Though many of the patterns identified recur in the information warfare literature, our designation of cyber-terrorism as requiring a physically destructive quality means that a full discussion on this topic lies beyond the remit of this chapter.

Perhaps the central question that should guide our examination of the effect of cyber-terrorism on public confidence is – *confidence in what or whom*? The obvious response is likely to be confidence in the government. But even this can be broken down by *actor* (confidence in the president; confidence in the national security apparatus; confidence in the government as an institution) or by *means* (confidence in the government's ability to protect the country against security threats; confidence in the government's general effectiveness). A sub-set of this classification that is often raised when discussing terrorism and public opinion is the 'rally round the flag' effect, which relates to short-term spikes in support for a country's leaders following an international attack. The short-term / long-term focus adds a temporal factor to the connection between exposure and confidence, though it also adds additional risks by conflating support and confidence.

We direct our analysis to consider how cyber-terrorism interacts with public confidence in leaders – otherwise known as the rally effect. In the immediate aftermath of the 9/11 attacks, approval ratings for President George W. Bush soared to 90% (Hetherington and Nelson, 2003). This became the archetypal example of the rally round the flag effect, a phenomenon that had been formally introduced by John Mueller in the 1970s. The rally round the flag theory identified a sharp (yet short-term) spike in approval and trust in a country's president in circumstances that met specific criteria: a sudden and international event taking place on the international level that is relevant to society as a whole, and that involves the direct participation of the president in solving the problem vis-à-vis a personified 'other'. Political psychology has a clear role to play in these circumstances since in "instances of sudden, dramatic, and international conflict, the salience and intensity of emotional appraisal, particularly the feelings of anger or anxiety, become the primary bases for evaluating government" (Ojeda, 2016, p. 76). Applying this well-developed theory to the case of cyber-terrorism provides an opportunity to explore how the cyber quality of the attacks alters the core theoretical mechanism. Kertzer, Oppenheimer and Zeitzoff (2020) sought to do just that by conducting a novel survey experiment and analyzing an original dataset of public opinion polls that followed publicly acknowledged cyber attacks against United States targets. The research team theorized that, in contrast to conventional terrorism, cyber-

threats would activate higher levels of anxiety due to the difficulty in identifying the attacker and the sense of omniscience surrounding cyber actors. The authors propose an 'uncertainty-distrust mechanism' according to which cyber-attacks corrode public confidence - a theory that would upend the typical cohesion effect that underlies the rally phenomenon in the aftermath of conventional terror attacks. The data offered tentative support for this uncertainty mechanism. One the one hand, the results surprisingly revealed the presence of mild rally effects in the aftermath of cyber attacks against the U.S. Yet on the other hand, the results also exposed how cyber attacks significantly lower public confidence in the ability of governmental institutions to effectively respond to future cyber threats.

Looking at public confidence in the government's ability to defend against security threats, we can observe a contrasting trend, indicating a need for additional research. One study by Gross, Canetti and Vashdi (2017) in Israel compared the self-reported levels of confidence in the government's ability to defend critical infrastructure and personal data following simulated conventional-terror or cyber-terror attacks launched by Hamas. The results indicated no significant variance in levels of confidence between the conditions, indicating that cyber-terrorism and conventional terrorism will have comparable effects on public confidence. Another study by Matzkin, Gross and Canetti (2020) similarly exposed participants to simulated video clips of lethal and non-lethal cyber and conventional terrorism. Once again, the research found no evidence that confidence levels varied across exposure to different forms of terrorism. The authors posited that this uniform response was due to a consistent appraisal of threat in a way that offered a sense of control over the situation.

Both Matzkin and colleagues (2020; which relied on self-reported emotional measures) and Backhaus et al. (2020; which measured anxiety through physiological stress hormones such as cortisol) observed higher levels of anxiety than anger in respondents following exposure to cyber-terrorism incidents. This is noteworthy as rally effects and public confidence are typically fueled by anger. That cyber-terrorism is more closely associated with anxiety than anger supports the uncertainty-distrust mechanism proposal that the uncertainty inherent in cyber attacks will reduce support for incumbent leaders and government institutions.

1.3.2 – Cyber-Terrorism and Foreign Policy Attitudes

A key political outcome of interest that is often associated with exposure to terrorism and political violence is foreign policy attitudes in general, and support for retaliatory strikes in particular. The intuitive nexus between exposure to terrorism and these policy attitudes is that civilians who are exposed to political violence adopt attitudes in relation to the attackers – be it a demand for revenge, or a desire to end the violence. According to the shattered assumptions theory, for example, exposure to political violence causes feelings of vulnerability that people seek to overcome via defensive coping attitudes that translate to policy positions (Janoff-Bulman, 1992). Building on this theory, the stress-based model of political extremism developed by Canetti et al. (2014) suggested that exposure to violence leads to psychological distress and heightened threat perception, which in turn predicts the adoption of hawkish political attitudes. In relation to cyber-terrorism, we propose that a thorough account of the relationship between

exposure to cyber-terrorism and foreign policy attitudes will integrate contextual, psychological, and political variables. The relevant contextual variables pertain to the type of cyber-terror attack that is launched (lethal attacks vs. non-lethal attacks; attributed attacks vs. anonymous attacks), as well as the underlying context of security, digital proficiency and political efficacy that exposed individuals possess. As yet, two related research directions have emerged that look at exposure to cyber-terrorism and foreign policy preferences: 1) Exposure to cyber-terrorism and support for retaliatory strikes and militant attitudes; and 2) Exposure to cyber-terrorism and support for the use of cyber weapons specifically. As described below, most of the research reveals that exposure to cyber attacks leads to public demands for aggressive and escalatory responses. It is interesting to note that this diverges from research on the behavior of elites and security officials who tend to espouse restraint in the aftermath of cyber incidents (Schneider, 2017; Valeriano and Jensen, 2019).

Gross, Canetti and Vashdi (2016, 2017) published a seminal series of papers related to this topic. This was the first set of research that sought to empirically measure the effects of public exposure to cyber-terrorism under controlled experimental conditions. The key finding was that exposure to cyber-terrorism is sufficient to manifest heightened desire for retaliation, and even for physical military conflagrations. This was a formative discovery since cyber-attacks up until then were viewed as more of a nuisance, incapable of inflicting genuine terror or damage, and certainly unable to evoke demands for lethal, military retaliation. These papers laid the foundation to understand three key principles. First, that cyber-terrorism was severe enough to generate significant negative emotions at equivalent levels to those of conventional terror acts. Second, that such exposure was directly connected to the adoption of militaristic political positions and demands for physical retaliation. Third, that the family of intervening emotional variables was similar to those elicited by conventional terrorism (namely, threat perception, anxiety and anger).

Building on this foundation, other research has sought to refine a more precise psycho-political mechanism that distinguished cyber-terrorism from conventional terrorism. According to Shandler et al.'s (2020) Cyber Lethality Threshold Theory, only lethal cyber-terrorism triggers strong support for retaliation. In this way, we observe a *lethality-threshold* for cyber-terrorism effects, wherein the outcome of the attack must meet a minimum level of destructiveness to trigger emotional responses and produce political outcomes at levels akin to conventional terrorism. They explain the lethality threshold by theorizing that non-lethal cyber-terrorism is more associated with cyber-crime due to the fact that the absence of deadly consequences and the absence of an immediately identifiable perpetrator clouds the scope and intent of the attack – both of which are important indicators through which the public perceives an act as terrorism. This research also found that the mechanism underpinning support for retaliation is driven by a mediated model where exposure to terrorism causes anger, which in turn drives the political effects. In this way, cyber-terrorism resembles conventional terrorism. This paradoxical discernment of a distinct cyber-terrorism effect that operates according to the same psychological mechanism as conventional terrorism reveals the need for additional research to hone the precise elements of similarity and difference.

A second research direction has explored how exposure to cyber-terrorism influences support for the use of cyber weapons particularly. Implicit in this thematic direction are questions about cyber-escalation and the principle of retaliatory equivalence. Specifically, will exposure to cyber-terrorism trigger heightened support for retaliatory cyber attacks? Is such support predicated on a principle of retaliatory equivalence that has long underlined military and public support for military strikes? Are there particular types of cyber-terror attacks that justify different forms of retaliation? Echoing the earlier claim of a distinct cyber-terrorism effect, Kreps and Schneider (2019) persuasively argued that cyber domains are qualitatively different from conventional, and even nuclear, military domains such that support for escalation following attacks "can be defined more by the means used to create effects than the effects themselves" (p. 2). This argument suggests that it is the very nature of a cyber attack that will encourage particular types of retaliation, and not the consequences of the attack.

Shandler, Gross and Canetti (2020) extended this topic in a multi-country experiment that offered different forms of retaliatory options to respondents who were exposed to cyber and conventional terror attacks. They found that support for the use of cyber weapons to retaliate against cyber-attacks was consistently and significantly higher than support for the use of missiles and other conventional means. What was interesting in this analysis was that the heightened support for the use of cyber weapons dissipated almost entirely if the respondents were exposed to *lethal* cyber attacks. This signifies that support for cyber weapons is predicated on their perception as non-lethal or less threatening military options, and that exposure to destructive cyber attacks undercuts this perception, significantly diminishing its appeal.

A recurring comment in many of these studies is that the identity of the attacker will influence foreign policy preferences by altering the intervening effect of anxiety or anger. Focusing on attacker identity raises several research challenges, as it is difficulty to accurately ascribe a cyber attack to a concrete perpetrator. Even if the attack can be successfully attributed, there is myriad evidence of states sub-contracting their cyber operations to proxy groups (Lindsay, 2013; Valeriano and Maness, 2018). Jardine and Porter (2020) have attempted to isolate the effect of attacker provenance through a discrete choice experimental design that manipulates the level of certainty about the identity of an attacker. They conclude that the uncertainty about attacker identity can inhibit public support for aggressive foreign policy options. What is lacking from this and other studies on support for use of cyber weapons is a robust explanation about the psychological mechanisms underlying the support for escalation or cyber-retaliation. This is the next stage in the development of this line of research.

1.4 – Conclusion and Future Directions

The advent of cyber-terrorism poses a significant and growing threat to modern society. This chapter asserts that neither individual psychology nor political context alone is sufficient to explain the effects of cyber-terrorism, and that a political psychology approach is needed to guide our analyses. Having reviewed the budding empirical literature, we find that individual exposure to cyber-terrorism causes shifts in political attitudes through intervening mechanisms

comprising emotional distress. Both the emotional intervening variables and the subsequent political outcomes bear similarities to those following exposure to conventional terrorism, although the direction and strength of these effects vary. This variance reflects the unique features of cyber-terrorism and affirms the need to adopt new psycho-political models.

Cyber-terrorism is still a nascent phenomenon. Only in the last decade have systematic empirical studies begun to explore the political effects of cyber-terrorism. In this short time, several robust and empirically tested theories have emerged that can help us understand this phenomenon. Shandler et al. (2020) confirmed a lethality threshold for cyber-terrorism wherein the emotionally-driven political effects are only activated when the cyber terror attack causes lethal consequences. Kertzer, Oppenheimer and Zeitzoff (2020) introduced an 'uncertainty-distrust mechanism' according to which cyber-threats cause public confidence to erode, in contrast to the typically cohesive effect of conventional terror attacks. Kostyuk and Wayne (2020) drew on psychological theories of risk perception to explain public behavior that is inconsistent with self-reported concern, while Gomez and Villar (2018) presented a mechanism that explains how uncertainty in the cyber realm activates incorrect cognitive heuristics leading to erroneous decision making. Yet despite these theoretical advances, the relative youth of the field means that the literature has yet to cover the full spectrum of political effects or emotional variables, nor tap into the full range of methodological tools. With this in mind, we conclude by marking five research foci and methodological instruments that can advance this budding field.

First, the initial empirical research on cyber-terrorism has understandably centered on a narrow range of intervening emotional variables that draws from established terrorism models. More than half of all research on cyber-terrorism highlights the role of anxiety and anger, with a smaller number of projects pushing the boundaries by exploring the emotions of dread and threat perception. While these findings offer a strong theoretical foundation, we encourage future research to consider additional intervening variables that relate to the specific qualities of cyber-terrorism. These include disgust and surprise as persuasively postulated by McDermott (2019), and apathy and shame as suggested by Bada and Nurse (2018) and Nurse (2018). Likewise, the political outcomes are limited to a small number of variables pertaining to foreign policy attitudes and public confidence. The next phase in research should consider additional political outcomes. One possibility is support for government regulation of cyberspace and cybersecurity regulations. Studies by Snider et al. (2020) and Cheung-Blunden et al. (2019) have begun to touch on the topic of cybersecurity preferences in the aftermath of cyber attacks, and in doing so has laid out a strong research agenda. Another promising direction is to consider political *behavior* in response to cyber-terrorism, and not just attitudes.

Second, the vast majority of research up until now has focused on civilian exposure to cyber-terrorism. The next steps should focus on the political psychology of perpetrators. We acknowledge that such an endeavor is highly challenging due to the difficulty of access and the inherent violence of terror perpetrators. Initial steps in this direction have been taken by Lee et al. (2020) who adapted space transition theory to the case of cyber-terrorists to explain the non-conforming behavior of terrorists as they transition from a physical space to cyberspace. Holt et al. (2017) and Kruglanski (2019) have begun to consider the correlates of participation in cyber-terrorism and the factors that influence individual willingness to conduct attacks.

Third, from a methodological perspective, we encourage future studies to incorporate physiological measurement techniques to gauge emotional states. The use of physiological measures in recent years by researchers such as McDermott and Hatemi (2014) and Canetti et al. (2014) has considerably advanced our understanding of the mechanisms underlying exposure to political violence. While studies measuring salivary cortisol have begun to proliferate in relation to cyber-terrorism (Backhaus et al. 2020; Canetti et al. 2017), there is still much work to do to understand the underlying physiological responses to cyber threats.

Fourth, we urge researchers to consider both theoretical and practical mechanisms that can minimize the negative political effects of cyber-terrorism by intervening at the emotional level. "In times of stress and threat, there is a strong need to reduce uncertainty by creating a comprehensible and coherent environment that provides a meaningful picture of traumatic events" (Canetti, 2017, p. 941). Hua, Chen and Luo (2018), for example, explore the antecedents of resilience to cyber terror attacks on financial infrastructure and concludes with concrete strategies to foster resilience. Similarly, Gomez and Villar (2018) propose potential organizational solutions to mitigate feelings of dread.

Last, we applaud the creativity of researchers who, in the absence of real-world destructive cyber attacks, have introduced a resourceful array of experimental processes such as video-clips and vignettes to simulate cyber-terrorism incidents. As the field matures, researchers will need to adopt other robust experimental manipulations such as natural experiments, quasi experiments and additional controlled randomized experiments that more closely reflect cyber-terrorism events. Some early multidimensional research that reflect more sophisticated experimental treatments include war game simulations run by Jensen and Valeriano (2019), Gomez and Whyte (2020b), and Schneider (2017), as well as survey experiments by Kreps and Schneider (2019), yet the field would benefit from more multifaceted empirical research.

We conclude with the following message. Cyber-terrorism has long been regarded as the next big threat. Though we refrain from echoing the exaggerated predictions of cyber-Armageddon that proliferated in the past, we do anticipate that more limited acts of destructive cyber-terrorism are likely to occur in the future. When such attacks do occur, we will need to understand how people will respond. The objective of a political-psychology approach is to recognize the human dimension of cyber-terrorism while still considering the larger political effects. Each person possesses a unique dispositional composition of character traits, resilience, emotional temperaments and reactivity to negative outcomes. These intervening psychological variables are the key to understanding how exposure translates to political behaviors and attitudes.

1.5 – References

Applegate, Scott D. 2013. "The dawn of kinetic cyber". *In Cyber Conflict (CyCon), 2013 5th International Conference* (pp. 1-15). IEEE.

Backhaus, S., Canetti, D., Gross, M., Waismel-Manor, I., Cohen, H. (2020) A Cyberterrorism Effect? Emotional Reactions to Lethal Attacks on Critical Infrastructure. Cyberpsychology, Behavior, and Social Networking (forthcoming).

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *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).

Bleich, Avraham, Marc Gelkopf, and Zahava Solomon. 2003. "Exposure to terrorism, stress-related mental health symptoms, and coping behaviors among a nationally representative sample in Israel." *Jama* 290, no. 5: 612-620.

Bonanno, George A., and John T. Jost. 2006. "Conservative shift among high-exposure survivors of the September 11th terrorist attacks." *Basic and Applied Social Psychology* 28, no. 4: 311-323.

Canetti, D. (2017). Emotional distress, conflict ideology, and radicalization. *PS: Political Science & Politics*, *50*(4), 940-943.

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

Canetti, D., Russ, E., Luborsky, J., Gerhart, J. I., & Hobfoll, S. E. (2014). Inflamed by the flames? The impact of terrorism and war on immunity. *Journal of Traumatic Stress*, *27*(3), 345-352.

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. *The political psychology of terrorism fears*, 193-212.

Canetti-Nisim, D., Halperin, E., Sharvit, K., & Hobfoll, S. E. (2009). A new stress-based model of political extremism: Personal exposure to terrorism, psychological distress, and exclusionist political attitudes. *Journal of Conflict Resolution*, *53*(3), 363-389.

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

Chanley, V. A. (2002). Trust in Government in the Aftermath of 9/11: Determinants and Consequences. Political Psychology, 23(3), 469–483.

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.

Cheung-Blunden, V., & Ju, J. (2016). Anxiety as a barrier to information processing in the event of a cyberattack. *Political Psychology*, *37*(3), 387-400.

Denning, Dorothy E., "A View of Cyberterrorism Five Years Later," in Internet Security: Hacking, Counterhacking, and Society, ed. K. Himma (Sudbury, MA: Jones and Bartlett Publishers, 2007), 124.

Denning, D. E. (2000). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. Focus on Terrorism, 9.

Denning, D. E. (2009). Barriers to entry: are they lower for cyber warfare?. *IO Journal*, *1*(1), 4.

Dunn Cavelty, M. (2019). The materiality of cyberthreats: securitization logics in popular visual culture. *Critical Studies on Security*, *7*(2), 138-151.

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

Egloff, Florian. (2020). Intentions and Cyberterrorism. In book: Oxford Handbook of Cyber Security. Oxford University Press

Eun, Yong-Soo & Judith Sita Aßmann (2016) Cyberwar: Taking stock of security and warfare in the digital age. *International Studies Perspectives* 17(3), 343-360.

Fischer, Agneta H., and Ira J. Roseman. 2007. "Beat them or ban them: The characteristics and social functions of anger and contempt." *Journal of personality and social psychology* 93, no. 1: 103.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” International Security 38, no. 2 (2013): 41–73. http://dx.doi.org/10.1162/isec_a_00136.

Gomez, M. A., & Villar, E. B. (2018). Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. Politics and Governance, 6(2), 61-72.

Gomez, Miguel and Whyte, Christopher. (2020a) “Cyber Malaise: The Effects of Extended Exposure to Cybersecurity Incidents”. Working paper.

Gomez, M. A. & Whyte, C. (2020b). Cyber Wargaming: Grappling with Uncertainty in a Complex Domain. Defense Strategy & Assessment Journal, 10 (1), 95 – 135.

Gomez, M. (2020). *Strategic Preferences in Cyberspace: A Cognitive-Cultural Approach*. Working paper.

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

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.

Halperin, Eran, Alexandra G. Russell, Carol S. Dweck, and James J. Gross. 2011. "Anger, hatred, and the quest for peace: Anger can be constructive in the absence of hatred." *Journal of Conflict Resolution* 55, no. 2: 274-291.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Heller, Aron. Israeli cyber chief: Major attack on water systems thwarted. *Washington Post*. 28 May 2020. 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

Hetherington, Marc J. and Michael Nelson. 2003. “Anatomy of a Rally E↵ ect: George W. Bush and the War on Terrorism.” PS: Political Science & Politics 36(01):37–42.

Holt, T. J., Kilger, M., Chiang, L., & Yang, C. S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. Deviant behavior, 38(3), 356-373.

Hua, J., Chen, Y., & Luo, X. R. (2018). Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. *Information & Management*, *55*(7), 928-938.

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.

Janoff-Bulman, Ronnie. 1992. Shattered Assumptions: Towards a New Psychology of Trauma. New York: Free Press.

Jardine, E., & Porter, N. D. (2020). Pick Your Poison: The Attribution Paradox in Cyberwar. Retrieved from osf.io/preprints/socarxiv/etb72

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. European Journal of International Security, 2(1), 64-87.

Jensen, B., & Valeriano, B. (2019). Cyber Escalation Dynamics: Results from War Game Experiments International Studies Association, Annual Meeting Panel: War Gaming and Simulations in International Conflict March 27, 2019.

Kertzer, Joshua D., Harry Oppenheimer, and Thomas Zeitzoff. "Do Cyberattacks Corrode?: Cyberattacks and Domestic Politics." Working Paper. 2020.

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

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.

Kruglanski, Arie. (2019, October). *What Prevents Cyber-Terrorism? The Psychology of a Puzzle*. Paper presented at the International Cyber-Terrorism Symposium, Haifa, Israel.

Lachow, I. (2009). Cyber-terrorism: Menace or myth. Cyberpower and national security, 434-467.

Lawson, S. T. (2019). *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge.

Lee, CS., Kyung-Shick, C., Shandler, R., Kayser, C. (2020) "Mapping Global Cyber Terror Networks: An Empirical Study of Al-Qaeda and ISIS Cyber-terrorism Events". Working paper.

Lerner JS, Keltner D. (2001). "Fear, anger, and risk." Journal of Personality and Social Psychology 81:146–59.

Lewis, C. W. (2000). The Terror that Failed: Public Opinion in the Aftermath of the Bombing in Oklahoma City. Public Administration Review, 60(3), 201-210.

Lindsay Jon R. 2015. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1, no. 1:53-67.

Lindsay, J. R. (2013, April). Proxy Wars: Control Problems in Irregular Warfare and Cyber Operations. In *International Studies Association anual meeting, San Francisco,(April 2013). http://www. jonrlindsay. com/papers*.

Macdonald, S., Jarvis, L., & Nouri, L. (2015). State cyberterrorism: a contradiction in terms?. *Contemporary Voices: St Andrews Journal of International Relations*, *6*(3).

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2020). A tale of two cybers-how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, 1-20.

Matzkin S., Gross, M., Canetti, D. (2020) Affect-as-Information and Appraisals in Public Confidence after Cyberterror. A Structural Equations Framework. Working Paper.

McCarthy, Justin. Americans Cite Cyberterrorism Among Top Three Threats to U.S. *Gallup.* 10 February 2016. https://news.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx

McDermott, R. (2019). Some emotional considerations in cyber conflict. *Journal of Cyber Policy*, 1-17.

McDermott, R., & Hatemi, P. K. (2014). The study of international politics in the neurobiological revolution: A review of leadership and political violence. *Millennium*, *43*(1), 92-123.

McDermott, Rose. 2010. "Decision making under uncertainty." *Proceedings of a Workshop Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. National Academies Press, Washington, DC: pp. 227–241.

Merolla, Jennifer L., and Elizabeth J. Zechmeister. 2009. Democracy at risk: How terrorist threats affect the public. University of Chicago Press.

Neria, Yuval, Laura DiGrande, and Ben G. Adams. 2011. "Posttraumatic stress disorder following the September 11, 2001, terrorist attacks: A review of the literature among highly exposed populations." *American Psychologist* 66, no. 6: 429.

Nurse, J. R. C. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In A. Attrill-Smith, C. Fullwood, M. Keep, &D. J. Kuss (Eds.), Oxford handbook of cyberpsychology (2nd ed.). Oxford: OUP https://doi.org/10.1093/oxfordhb/9780198812746.013.35.

Norman, Jim. North Korea, Cyberterrorism Top Threats to U.S. *Gallup.* 5 March 2018. https://news.gallup.com/poll/228437/north-korea-cyberterrorism-top-threats.aspx

Nye, J. S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4), 18-38.

Ojeda, C. (2016). The effect of 9/11 on the heritability of political trust. *Political psychology*, *37*(1), 73-88.

Sanger, David E. 2018. "Russian Hackers Appear to Shift Focus to U.S. Power Grid." *New York Times,* July 27, 2018.

Schneider, J. (2017, March). Cyber and crisis escalation: insights from wargaming. In *USASOC Futures Forum*.

Shandler, R., Gross, M., Backhaus, S., Canetti, D. 2020. Cyber Terrorism and Public Support for Retaliation - A Multi-Country Survey Experiment. Working paper. Available at: https://sites.google.com/view/ryanshandler

Shandler, R., Gross, M., Canetti, D. 2020. A Tenuous Public Preference for Cyber Weapons. Working paper. Available at: https://sites.google.com/view/ryanshandler

Silver, Roxane Cohen, E. Alison Holman, Daniel N. McIntosh, Michael Poulin, and Virginia Gil-Rivas. 2002. "Nationwide longitudinal study of psychological responses to September 11." *Jama* 288, no. 10: 1235-1244.

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security, 41*(3), 72-109.

Slone M, Shoshani A. Evaluation of preparatory measures for coping with anxiety raised by media coverage of terrorism. Journal of Counseling Psychology 2006; 53(4):535.

Snider, K., Zandani, S., Shandler, R., Canetti, D. 2020. Cyber Attacks, Cyber Threats and Attitudes toward Cybersecurity Policies. Working paper.

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

Sunstein, C. R. (2009). *Worst-case scenarios*. Harvard University Press.

Valeriano, B. G., & Jenson, B. (2019). The Myth of the Cyber Offense: The Case for Cyber Restraint. *Cato Institute Policy Analysis*, (862).

Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. *The Oxford Handbook of International Political Theory*, 259.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.

Valeriano, B., & Gomez, M. A. (2020). The failure of academic progress in cybersecurity. *Council on Foreign Relations Blog.* Available at: www.cfr.org/blog/failure-academic-progress-cybersecurity.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559.

Wayne, Carly. 2019. Risk or Retribution: The Micro-foundations of State Responses to Terror (Doctoral dissertation).

Zetter, Kim. 2015. "A Cyber Attack Has Caused Confirmed Physical Damage for the Second Time Ever." *Wired*, August 1, 2015.