Article

Social Science Computer Review
2015, Vol. 33(4) 479-497
© The Author(s) 2014
Reprints and permission:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/0894439314546815
ssc.sagepub.com
SAGE

Exploring Reactions to Hacktivism Among STEM College Students: A Preliminary Model of Hacktivism Support and Resistance

Lisa M. PytlikZillig[1], Shiyuan Wang[1], Leen-Kiat Soh[2], Alan J. Tomkins[1], Ashok Samal[2], Tonya K. Bernadt[3], and Michael J. Hayes[3]

Abstract

This study investigated the predictors of support for and resistance to hacktivism in a sample of 78 science, technology, engineering, and mathematics majors at a Midwestern university. Results from surveys about real-world instances of hacktivism indicate different preexisting global attitudes predict specific situational hacktivism support (predicted by admiration) versus resistance (predicted by willingness to report). Also, participants gave greater weight to their perceptions of hacktivist (rather than target) trustworthiness/untrustworthiness. Comparisons among different facets of trustworthiness suggest perceptions of shared values with and integrity of the hacktivists are especially important for predicting support and resistance. Participants also were more supportive of hacktivism rated as having higher utilitarian value but not less supportive of hacktivism initiated for retribution. Mediation analyses indicated that situation perceptions significantly mediated the effects of global attitudes on hacktivism support/resistance, but that the significance of specific mediators was inconsistent across analyses. This suggests that the importance of mediators may depend on specific context.

Keywords

hacktivism, motives, trust, distrust, shared values, attributions, attitudes

Introduction

Even our most basic infrastructure depends on cyber systems and components that could be hacked and sabotaged with potentially large-scale, life-threatening consequences (Holt & Kilger, 2012),

[1] University of Nebraska Public Policy Center, Lincoln, NE, USA
[2] Department of Computer Science & Engineering, University of Nebraska–Lincoln, Lincoln, NE, USA
[3] University of Nebraska–Lincoln National Drought Mitigation Center, Lincoln, NE, USA

Corresponding Author:
Lisa M. PytlikZillig, University of Nebraska Public Policy Center, 215 Centennial Mall South #401, Lincoln, NE 68508, USA.
Email: lpytlikz@nebraska.edu

making hackers a primary threat to national security. There are many motivations behind hacking, including the so-called "white hat" motives such as increasing knowledge or improving security, "black hat" motives such as personal gain or retribution, and "gray hat" motives such as curiosity or challenge (Xu, Hu, & Zhang, 2013). *Hacktivism*, the subject of this article, is defined as unauthorized or illegal electronic disruptions or intrusions motivated by activist purposes, especially for advancing political causes (Denning, 2001; Manion & Goodrum, 2000). Thus, "hacktivists" are distinguished within the broader category of hackers by their use of technology and hacking as means to achieve political purposes or "greater good" (Taylor, 2005). Hacktivism is an important area of study because hacktivist motives stemming from social, political, economic, and cultural (SPEC) conflicts are increasingly cited as reasons why hacker groups plan and execute their attacks (Gandhi et al., 2011; Holt & Kilger, 2012).

While there is an emerging literature base on hacktivism (e.g., Denning, 2001; Jordan & Taylor, 2004; Manion & Goodrum, 2000; Taylor, 2005), there is still a gap in pinpointing the factors influencing public perceptions and support for or resistance to hacktivism. This gap is important because, to a large extent, hacktivists cannot achieve their aims without public support. Hacktivists have a unique and polarized social standing that distinguishes them from cybercriminals with other motives. Rather than hiding their activities, hacktivists intend their actions to be public and recruit public support. Thus, onlookers can also impact cybersecurity by their actions supporting or resisting ongoing hacktivism attacks. Mass action hacktivism, for example, may simply require onlookers to visit a site or click on a link. Such mass action hacktivism does not require onlookers to have much skill but to succeed, does require supportive onlookers to take action. Also, unskilled supporters can be and have been encouraged to help with attacks through the provision of tools and tutorials (Holt & Kilger, 2012; Jordan & Taylor, 2004). Because hacktivism can include activities ranging from technologically unsophisticated behaviors such as trolling and launching verbal attacks (Workman, Phelps, & Hare, 2013), to more technologically sophisticated attacks on systems (see Jordan & Taylor, 2004, for an in-depth review), "onlookers" can relatively easily be transformed into active hacktivists. Thus, learning about the factors that predict onlooker support for and resistance to hacktivism may also advance understanding of how hacktivism is spread or prevented. Also, because technologically unsophisticated "normative" forms of hacktivism are predictive of technically sophisticated, "nonnormative" forms (Workman et al., 2013), lessons learned about less-sophisticated onlookers who are at risk to become attackers may inform understanding of sophisticated attackers.

As Holt and Bossler (2014) note in their review, research specifically examining hacktivist motives or onlooker attitudes toward "hacktivities" is rare. Providing one example of such research, Gandhi and colleagues (2011) analyzed the SPEC motives underlying historically recorded cyberattacks and created a taxonomy of motives ranging from retaliation and political dissatisfaction (political motives), to land and cultural disputes (sociocultural motives), to financial gain (economic motive). Relatedly, Samuel (2004) interviewed hacktivists and analyzed secondary material to develop a typology of hacktivist activities including (1) *performative hacktivism*, which may take the form of digital sit-ins and is conceptually closest to civil disobedience, (2) *political cracking*, which is unique in its disregard for the law and may be conceptually closest to cyberterrorism, and (3) *political coding*, which involves creation of software code to achieve political ends. These three forms vary in orientations toward illegal activity (cracker hacktivists are most accepting) and reliance on technical expertise (performative hacktivists are least technically sophisticated). Both Gandhi et al.'s and Samuel's work are important to understanding the variety of hacktivists and hacktivism in existence but do not directly address how onlookers might react to different forms of hacktivism or whether the same dimensions would be important when thinking about not only those who initiate hacktivist attacks but also onlookers who then support (or resist) the attacks.

Somewhat more relevant is research by Holt and Kilger (2012). They used a diverse sample of college students from a Midwestern university to compare domestic and international students' (all

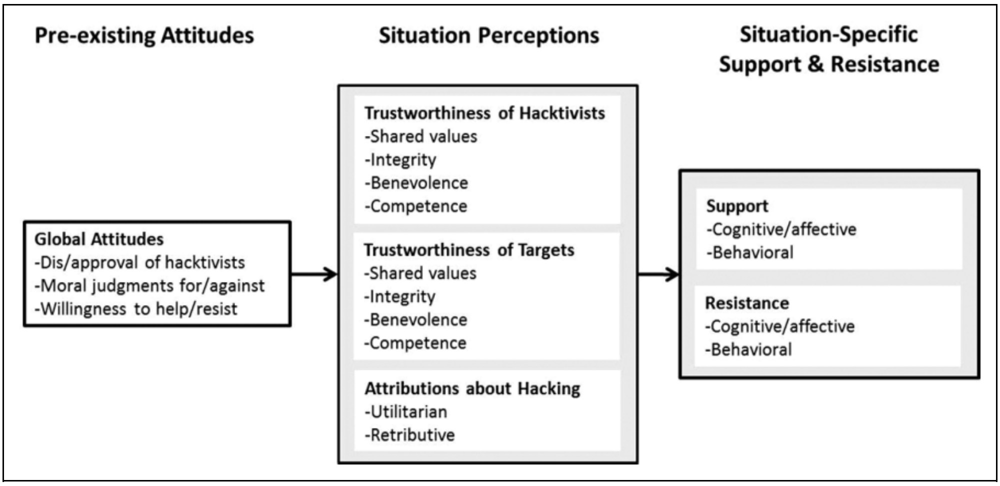

Figure 1. Overview of preliminary model of hacktivism support and resistance.

studying within the United States) endorsement of politically motivated cyberattacks against government and critical infrastructure targets. Using scenario stimuli, they investigated the predictors of self-reported willingness to take specific physical (e.g., write a letter, damage a government building) or online (e.g., post to social networking sites and deface target websites) actions against the students' own or another (fictitious) nation. Holt and Kilger's findings indicate that, of the variables they examined—which included patriotism, nationalism, attitudes toward group equality and outgroups, technological skill, history of digital piracy, and demographics—willingness to engage in *physical* (offline) protests were by far the best predictors of willingness to engage in *online* protests. In addition, a history of digital piracy (and, less reliably, out-group antagonism) also predicted willingness to engage in cyberattacks. Given that their participants were students, not hacktivists, these results may reflect sources of onlooker support for the forms of online protest investigated. However, we found no research directly examining onlooker's willingness to support or resist hacktivism.

Our research begins to fill this gap in the literature and more generally add to the literature uncovering "the dynamics by which individuals come to participate in protest" (Schussman & Soule, 2005, p. 1084)—in this case, participation in protests through support of ongoing hacktivism. As we detail in the next sections, we especially seek to illuminate proximate psychological factors that may impact individual support of or resistance to hacktivist activities. Specifically, as illustrated in Figure 1, we explore different types of cognitive/affective and behavioral support and resistance, and the potential roles of preexisting attitudes toward hacktivism and situational perceptions (e.g., of the actors, targets, and the effects of the actors actions) in predicting that support and resistance.

Dependent Variables: Situation-Specific Hacktivism Support and Resistance

Because we were interested in motivation, we defined our primary dependent variables, support for and resistance to hacktivism (Figure 1, rightmost variables), not only in terms of *behavioral* support and resistance but also in terms of supportive and resistant cognitions and affects, which might lead to overt behavioral support and resistance. Such an approach is consistent with long-standing theories of attitudes such as the Theory of Reasoned Action (Ajzen, 1991, 2001; Ajzen & Fishbein, 1980), which posits that behavioral intentions are driven by cognitive and affective evaluations of the expected likelihood and value of various outcomes.

We thus created a measure of proximal and situation-specific but generally stated behavioral intentions and cognitive/affective indicators of hacktivism support and resistance. The situation-specific focus was very intentional, as we are interested in support and resistance behaviors that occur in concrete situations containing features that may impact people's behaviors separately from their personal and more stable attitudes (which we also assessed, as discussed subsequently). On the other hand, our measures were general in the sense that we did not specify *how* the respondent might help (as did, e.g., Holt & Kilger, 2012), because we intended the measures to be applicable across specific contexts and to persons of different skill levels. By assessing behavioral intentions separately from cognitions/affects, we kept the hypothesized underlying psychological components of support and resistance separate from behaviors and behavioral intentions.

Potential Predictors: Preexisting Global Attitudes Toward Hacktivism

The first elements of our preliminary model predicting hacktivism support and resistance were preexisting global attitudes (Figure 1, leftmost variables). In general, *attitudes* are evaluations of objects that can be held in thought (Bohner & Dickel, 2011) and are typically described as ranging from positive to negative (e.g., good/bad, beneficial/harmful; Ajzen, 2001). Attitudes show characteristics of both stability and change and are influenced by associated cognitive beliefs and expectancies, affective feelings and values as well as contextual factors (Bohner & Dickel, 2011). We surmised that just as personality traits (overall tendencies to behave in certain ways over time) are predictive of behaviors in a specific situation (e.g., Fleeson, 2007), attitudes reflecting support of or resistance to hacktivism *generally* (i.e., global attitudes toward hacktivism) will also be predictive of evaluations that people construct in specific situations (e.g., hacktivism support/resistance). Thus, our first hypothesis was:

> **Hypothesis 1:** Preexisting global attitudes toward hacktivism will be predictive of situation-specific hacktivism support and resistance.

Such distinctions between more global versus situation-specific constructs have also been made in other attitude studies (e.g., Gau, 2013). We assessed global attitudes toward hacktivism support and resistance similar to how we assessed situation-specific support and resistance: by asking participants about their affective (e.g., admiration), cognitive (e.g., moral judgments), and behavioral (e.g., willingness to help or to report) reactions to hacktivism *in general*. Assessing such attitudes is also consistent with literature pertaining to hacktivism. For example, some have discussed admiration for hacktivists (Levy, 2001), and others have pointed to the importance of moral judgments for determining which computer-savvy individuals become hackers and which do not (Xu et al., 2013). As illustrated in Figure 1, while we hypothesized that these attitudes would importantly predict support and resistance, we expected their effects to be mediated by situational perceptions, which we discuss next.

Potential Mediators: Trust and Distrust

A second class of elements in our model includes perceptions of trustworthiness and untrustworthiness. We were particularly interested in these perceptions because hacktivists are often characterized as having high distrust in their targets (Levy, 2001; Warren, 2008; Yar, 2005). Indeed, although as previously noted more recent usage of the term "hacking" encompasses a wide range of characters and actions, "old school" definitions of hacking implied a certain "ethic" of protest and "distrust of political, military and corporate authorities" (Yar, 2005, p. 389) resembling contemporary descriptions of hacktivists. Despite this emphasis, research on the role of trust or distrust as a precursor to or motivation for hacktivism or for *supporting* hacktivism is lacking. For onlookers, their trust and distrust of, not only the targets, but also the hacktivists who initiate attacks, may also play an important role in motivating their support or resistance.

Dimensions of perceived trustworthiness identified by prior research have included judgments of benevolence, integrity, competence (Mayer, Davis, & Schoorman, 1995; PytlikZillig, Tomkins, Herian, Hamm, & Abdel-Monem, 2012), and shared values (Siegrist, Cvetkovich, & Roth, 2000). In the present study, we assessed these specific perceptions of trustworthiness in order to test for the potentially different effects of each and investigate the following hypotheses and research question:

> **Hypothesis 2:** Trustworthiness and untrustworthiness of the *targets* of hacktivism will predict resistance and support for the hacktivism, respectively.
>
> **Hypothesis 3:** Trustworthiness and untrustworthiness of the *hacktivists* will predict support for and resistance to the hacktivism, respectively.
>
> **Research Question 1:** Are specific facets of trustworthiness and untrustworthiness more strongly related to hacktivism support or resistance than other facets?

Potential Mediators: Hacktivism for Retributive Versus Utilitarian Purposes

The next component of our model involved attributions about the purpose and effects of the hacktivism activities. Attribution theory (Hareli & Weiner, 2002; Weiner, 1985, 2010) identifies dimensions by which persons assign causality as they interpret the world around them and links those attributions to motivations, emotions, and behaviors. Each of the motives identified by Gandhi et al. (2011, p. 36), for example, can be evaluated on two attribution dimensions, namely retribution (e.g., retaliation against acts of aggression) and utility (e.g., cyber-espionage). Prior research and theory suggest people perceive actions attributed to *retributive motives* as more hostile and less moral than utilitarian/instrumental actions (Feshbach, 1970; Kanekar, Bulsara, Duarte, & Kolsawalla, 1981). Based on this prior work and theory, we examined the effects of perceiving hacktivism as retributive and/or utilitarian on hacktivism support and resistance and hypothesized that:

> **Hypothesis 4:** Perceptions of the retributive value of the hacktivism will negatively predict support and positively predict resistance, while perceptions of the utilitarian value will have the opposite effects.

Finally, to begin to draw potentially causal connections between the variables in our preliminary model of hacktivism support and resistance (specifically, the connections implying mediation outlined in Figure 1), we sought to answer the following research question:

> **Research Question 2:** Do situation-specific perceptions mediate the impacts of preexisting global attitudes on hacktivism support and resistance and, if so, which perceptions are the most important mediators?

The Present Study

We investigated our hypotheses and research questions among those likely to be among the future population of potential hacktivist supporters: undergraduates majoring in STEM fields (Yar, 2005). To establish a greater understanding of how STEM students view hacktivism, we asked participants to complete items assessing general attitudes toward hacktivism and then to respond to examples of real-world instances of hacktivism. Following completion of the surveys assessing perceptions of the instances of hacktivism, participants engaged in a discussion about ethics in computer science designed to fulfill course-related ethics requirements.

Method

Participants

The survey was part of required course activities but participants could choose to withhold consent for analysis of their responses. A total of 78 (92%) of 85 students completing the survey for course credit consented for their data to be used in this research. All participants were students in a computer science course for engineers at a Midwestern university, ranging in age from 18 to 22 years ($M = 19.45$, $SD = 1.05$) and 82% were male. Most were freshmen (40%) or sophomores (41%), and White (89%). Politically, 49% identified as Republicans, 19% as Democrats, and 32% Independent. All students in the course reported science, technology, engineering, or math (STEM) majors and, for most (91%), this was their first computer science course.

Procedures

The survey was administered online as homework. Participants were given the definition of hacktivism as "engaging in unauthorized online behaviors in order to achieve a greater purpose (e.g., a political purpose)." To distinguish hacktivism from hacking it was noted that, in contrast, "hacking is any unauthorized online behaviors, and may simply be for personal gain, and does not have to be engaged in for any greater purpose." Immediately after this explanation, participants answered the questions measuring their *global attitudes toward hacktivism* and some demographic questions.

Participants next read about real-world hacktivism-related events. Each scenario was briefly described for the students, the hacktivists and the targets were explicitly identified, and links were provided to online news articles describing the events (see online Appendix A[1]). All students first read about an instance of hacking involving the stealing and release of e-mails from climate scientists (climategate). Next, they reported their perceptions of the *trust- or untrustworthiness* of the climategate hacktivists and their targets (climate scientists), their perceptions of the hacktivist motives as *utilitarian* or *retributive*, and their support for and resistance to the hacktivism in that specific scenario (*situation-specific support* and *resistance*).

After responding to the climategate scenario, participants were randomly assigned one of three other real-world events. Use of different second scenarios was designed to create variation so that we might detect relationships between situation-specific perceptions and support for and resistance to hacktivism. The three scenarios included descriptions of (1) a video posted as incriminating evidence against teens at a party where a rape occurred (rape video), (2) Aaron Swartz's alleged hacking of JSTOR articles prior to his suicide (hacker suicide), and (3) the anonymous group's denial of service attacks and petition for such attacks to be considered legal forms of social protest (denial of service). Note that the four scenarios (climategate, rape video, hacker suicide, and denial of service) varied in terms of the likely trustworthiness of the targets (e.g., we expected climate scientist targets to be viewed as more trustworthy than teen bystanders to an ongoing rape) and, although not the primary focus of this study, also varied on dimensions identified by Samuel (2004). For example, the actions of the hacktivists in the climategate and denial of service scenarios involved potentially sophisticated hacking activities and might be classified as political cracking. Meanwhile, the use of the rape video to achieve justice for the rape victim may be viewed as performative hacking because it did not require sophisticated programming or hacking skills but was certainly a form of active protest.

After reading the second scenario, the same variables were assessed as had been after the climategate scenario. Finally, participants were asked to write brief preliminary answers to three open-ended questions (not analyzed here) that would prepare them for the in-class discussion.

Measures

Unless otherwise noted, all measures were accompanied by a 7-point Likert-type scale with responses ranging from *strongly disagree* to *strongly agree*. With the exception of the trust measures, our measures had not been used in prior studies. Therefore, we conducted a number of preliminary analyses including assessments of face validity of items, examination of internal reliabilities of scales and item-total and α-if-deleted values for individual items, and principal component analysis and exploratory factor analysis using principal axis factoring (described subsequently, with additional details in online Appendix B[1]). Furthermore, we cross validated our statistical results on a second sample from a related study, considering both sets of results in our decisions for final scale composition.

Hacktivism support and resistance. *Situation-specific hacktivism support* and *resistance* were assessed with 12 items divided into subscales based on whether items referred to behavioral versus cognitive/affective support or resistance. The distinction between support and resistance was made on the basis of theory suggesting that approach and avoidance behaviors and motives are fundamentally different, relying on different neural substrates (Corr, 2013; Gray, 1991). The division between cognitions/affects versus behaviors was based on theory suggesting that cognitions and affects precede and motivate behaviors (Ajzen, 1991, 2001; Ajzen & Fishbein, 1980). Although our factor analyses suggested two (support and resistance) rather than four factors, because of the exploratory nature of our study and the potential theoretical importance of distinguishing behavioral from psychological constructs, we kept them separate.

The final subscales were as follows: *behavioral support* (2 items, e.g., "If I were in a position to help with such hacking efforts, I would do so"; αs for this scale ranged from .78 to .97 across scenarios[2]), *behavioral resistance* (2 items, e.g., "If I knew someone was doing this hacking, I would try to tell the authorities"; αs = .76–.99), *cognitive/affective support* (3 items, e.g., "The behavior was morally right"; αs = .64–.91), *cognitive/affective resistance* (3 items, e.g., "I generally disapprove of this behavior in this case"; αs = .42–.86). For the mediation analyses, we combined all support items and all resistance items into *overall support* (6 items, αs = .75–.92) and *overall resistance* (6 items, αs = .77–.93) scales that each included an additional item assessing empathetic understanding or lack of understanding (e.g., "I cannot understand why anyone would ever engage in such behavior").[3]

Global attitudes toward hacktivism were assessed with 8 items. Based on exploratory factor analyses and face validity considerations, we created the following subscales: *admiration* (3 items, e.g., "I really look up to people who 'hack' for activism purposes (i.e., for a good cause)"; α = .85), *moral judgment* (3 items, e.g., "Hacking is always wrong, even if it is supposedly for a good cause"; α = .90), and *willingness to report* (2 items, e.g., "I'd report someone trying to hack a computer system, even if they were doing it for a cause that I believe in"; α = .85).

Trust/distrust in hacktivist or target. For each scenario, the trust/distrust constructs were assessed with regard to both the hacktivist and the target of the hacking. Most of the trustworthiness scales were comprised of one negative and two positive items constructed on the basis of prior research (e.g., Hamm et al., 2013; PytlikZillig et al., 2012). We assessed *unspecified trust* (3 items, e.g., "I trust/distrust the target/hacker"; αs ranged .66–.94 across scenarios), *benevolence/malevolence* (4 items for target, 3 items for hacker, e.g., "the target/hacker had good intentions"; αs = .68–.78), *competence/incompetence* (3 items, e.g., "they are competent at what they do," αs = .71–.95), *integrity/lack of integrity* (3 items, e.g., "they are persons of integrity"; αs =.46–.91), and *shared/unshared values* (3 items, e.g., "things that are important to me are also important to them"; αs = .76–.92).

Attributions. To assess perceptions of the effects of the hacktivism and likely hacktivist motives, we used two scales, namely *utilitarian motives/attributions* (3 items, e.g., "The hacking succeeds in giving access to information that should be public"; αs = .56–.88) and *retributive motives/attributions* (3 items, e.g., "The target got what he or she or they deserved"; αs = .58–.79). Although factor analyses of these items suggested a one-factor solution, we retained separate scales due to the exploratory nature of our study and the potential theoretical importance of the distinction between items.

Results

Between-Scenario Differences

Prior to examining our specific hypotheses, we first examined our measures' sensitivity to differences between scenarios. Given that we were using new measures, this was important to establishing the validity of our scales. Because every student had read and responded to the climategate scenario and one other randomly assigned scenario (a within-participant design), we used paired *t*-tests to compare the climategate scenario and each other scenario. For differences among the three other scenarios, we used between-group one-way analyses of variance (ANOVAs) with pairwise follow-up independent *t*-tests for differences whenever a significant omnibus difference was found.

As shown in Table 1, analyses revealed numerous differences between scenarios, supporting the validity of the scales. For example, comparisons on the situation-specific *hacktivism support* and *resistance* indicated that the most support and least resistance to hacktivism were for the rape video scenario. Meanwhile, the least support and most resistance to hacktivism were for the climategate scenario. The rape video scenario was significantly different from the climategate scenario on most of the hacktivism support/resistance scales. Also, there was significantly lower behavioral resistance in response to the denial of service scenario than to the climategate scenario. Between-group comparisons of the three between-group scenarios found an omnibus significant difference only for cognitive/affective support, $F(2, 75) = 5.77$, $p = .01$, $\omega^2 = .07$, with post hoc tests indicating a significant difference between the rape video and denial of service scenarios (with more cognitive/affective support for hacktivism in the rape scenario).

On the situation perception variables, comparisons between climategate and other scenarios revealed a number of differences. The climategate and rape video scenarios significantly differed on all *trust/distrust* subscales pertaining to the *targets* of the hacking: Participants' trust in the climategate target (climate scientists) was significantly higher than trust in the targets of rape video scenario (teen bystanders to the rape). Also, compared to climategate *hacktivists*, participants had significantly more trust in the rape video hacktivist's integrity and shared values, more trust in the suicide hacktivist's benevolence, competence, integrity, and shared values, and more trust in the denial of service hacktivists' competence. Compared to the climategate scenario, hacktivism in rape video scenario, and denial of service scenario were also rated higher for retributive motives but not utilitarian motives. Meanwhile, hacktivism in hacker suicide scenario was rated higher in utilitarian purposes than the climategate scenario.

Comparisons among the other three scenarios on the situation perception variables also revealed significant, moderate to large, $F(2,75) = 9.65$–30.26, ps < .01, $\omega^2 = .18$–$.50$, omnibus differences for all dimensions of trust/distrust in targets, and targets in the rape video scenario rated as least trustworthy. When it came to *trust/distrust* of the *hacktivists*, omnibus ANOVA results indicated significant differences only on the benevolence dimension, $F(2, 75) = 4.32$, $p = .02$, $\omega^2 = .08$, with the denial of service hacktivists rated as least benevolent.

Finally, examination of between scenario differences in *retributive and utilitarian attributions* also revealed significant omnibus differences on both dimensions, with moderate effect sizes, utilitarian $F(2, 75) =10.21$, $p < .001$, $\omega^2 = .12$; retributive $F(2, 75) =14.02$, $p = .00$, $\omega^2 = .24$, and a

Table 1. Between-Scenario Comparisons of Participant Ratings.

	Climategate $n = 78$		Rape Video $n = 29$		Hacker Suicide $n = 26$		Denial of Service $n = 23$	
	M	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*
Hacktivism support/resistance								
Overall support	3.40^{a}	.95	4.29^{b}	1.19	3.81^{a,b}	1.39	3.54^{a,b}	.73
Cognitive/affective support*	3.25^{a}	1.04	4.33^{b}	1.25	3.68^{a,b}	1.54	3.38^{a}	.75
Behavioral support	2.96^{a}	1.37	3.69^{b}	1.53	3.37^{a,b}	1.72	3.28^{a,b}	1.09
Overall resistance	4.25^{b}	.90	3.60^{a}	1.17	3.85^{a,b}	1.48	3.97^{a}	.78
Cognitive/affective resistance	4.61^{b}	.96	3.84^{a}	1.32	4.10^{a,b}	1.41	4.09^{a}	.80
Behavior resistance	4.18^{a}	1.11	3.60^{a}	1.35	3.75^{a}	1.80	4.11^{a}	1.07
Trustworthiness of targets								
Unspecified*	4.15^{b}	1.15	2.70^{a}	1.17	4.59^{b}	.95	4.22^{b}	.86
Benevolence*	4.42^{b,c}	.80	2.49^{a}	1.17	4.44^{c}	.82	3.87^{b}	.79
Competence*	5.00^{b}	.86	3.90^{a}	1.43	5.31^{b}	1.12	4.93^{b}	1.06
Integrity*	4.23^{b}	1.05	2.45^{a}	1.13	4.59^{b}	.95	4.22^{b}	.68
Shared values*	4.15^{b}	1.03	2.59^{a}	1.17	4.38^{b}	1.03	4.01^{b}	.79
Trustworthiness of hackers								
Unspecified	3.39^{a}	.93	3.78^{a}	.90	3.78^{a}	1.36	3.62^{a}	.79
Benevolence*	4.02^{a}	.88	4.74^{b}	.94	4.94^{b}	1.16	4.10^{a}	.98
Competence	5.00^{a}	.90	5.03^{a,b}	1.32	5.67^{b}	1.15	5.07^{a,b}	1.17
Integrity	3.25^{a}	.86	3.93^{b}	.80	3.67^{b}	1.33	3.57^{a,b}	.88
Shared values	3.45^{a}	.88	4.11^{b}	.85	4.00^{b}	1.48	3.65^{a,b}	.91
No care about impact	3.88^{b}	1.31	3.83^{a,b}	1.61	2.96^{a}	1.18	3.48^{a,b}	1.28
Hacker motives/hacktivism effects								
Utilitarian*	3.62^{a,b}	1.14	4.08^{b,c}	1.31	4.32^{c}	1.27	3.19^{a}	.68
Retributive*	3.30^{a}	1.07	4.85^{c}	1.06	3.36^{a,b}	1.43	3.65^{b}	.78

Note. Scales range from 1 to 7, with 4 = *neutral.*

*Indicates significant omnibus difference among the three between-group scenarios. Same superscripts indicate a lack of significant differences at the $p < .05$ level based on paired or independent group's t-tests as described in the text. If means within a row do not share a common superscript, then those means are significantly different from one another. For the between-group analyses, post hoc uncorrected t-tests were only conducted if the omnibus test was significant. The climategate reported *M* and *SD* is computed across all participants; there were no significant differences in the ratings of climategate between the three subgroups receiving different second scenarios.

logical pattern of differences (e.g., Schwartz's downloading activity was among the most utilitarian and least retributive scenarios).

Predicting Situation-Specific Hacktivism Support and Resistance

We next tested our hypotheses and explored the prediction of situation-specific support and resistance for hacktivism using hierarchical multiple regression analyses. Because these were exploratory analyses conducted on data from relatively small samples ($N = 78$ in climategate, $n = 23$–29 in the other three scenarios), instead of conducting multivariate analyses examining the prediction of all dimensions of situation-specific support at once, we separately examined the prediction of each dimension of situation-specific support. Specifically, we conducted four hierarchical regression analyses (one for each dependent variable) for the climategate scenario (which all students rated) and four for the other three scenarios (which were randomly assigned to students). To reduce the number of predictors, we conducted a number of exploratory analyses prior to the regression analyses. One option for these preliminary analyses was to conduct factor analyses of all of our predictor variables and reduce them to a smaller number of scales. However, our research question (which *specific* perceptions are most important for predicting the dependent variables [DVs]?) requires keeping individual perceptions separate. Therefore, we conducted a series of regression analyses, including both stepwise and simple simultaneous regression,[4] to examine which variables were most important from each of the three sets of key variables (i.e., separately examining general attitudes toward hacktivism, trust/distrust, and attributions). Then, using only the significant predictors from the stepwise regressions, we conducted a series of hierarchical regression analyses regressing each of our situation-specific hacktivism support/resistance outcome variables on the following predictors, in the following order for the climategate and other scenarios:

Climategate Scenario:	**Other Scenarios**:
Global attitudes toward hacktivism (step 1)	Global attitudes toward hacktivism (step 1)
Attributions (step 2)	Dummy codes for scenarios (step 2)
Trust/distrust in the target (step 3)	Attributions (step 3)
Trust/distrust in the hacktivists (step 4)	Trust/distrust in the target (step 4)
	Trust/distrust in the hacktivists (step 5)

Our procedures required individual variables to compete with one another in order to be included in the model and results in different specific predictors for different DVs. Thus, parameter estimates from one model are not comparable to parameter estimates from another model (because different control variables are included in each model). However, we were most interested in the pattern of results obtained and the reliability of that pattern across models, rather than specific parameter estimates.[5] The resulting patterns are reported in Table 2, which shows the specific predictors entered for each model, the variables that were significant when entered on their respective step (denoted by *), and the variables were still significant in the final model (boldface variables). A number of observations are apparent. First, relevant to our first hypothesis (Hypothesis 1), general attitudes toward hacktivism did predict support and resistance. Admiration for hacktivists was especially likely to predict support variables, and willingness to report hacktivism was especially likely to predict resistance to hacktivism. However, the moral judgment scale did not emerge as an important predictor in any of the analyses. Next, relevant to Hypotheses 2 and 3, as indicated by the direction of the effects (i.e., positive or negative directions of the effects) trust in the targets and distrust in the hacktivists did tend to predict support for or low resistance to hacktivism. It is also noteworthy that, as shown in Table 2, the variance accounted for by trust/distrust in the hacktivists was always greater than or equal to the variance accounted for by trust in the targets. Thus, it appeared that our participants were attending more to whether they trusted/distrusted the hacktivists, than to their distrust/trust of the targets, in making their decisions about support/resistance.

Relevant to Research Question 1 concerning the specific facets of trust/distrust that may relate to hacktivism support and resistance, results from the hierarchical regression analyses also pointed in particular to perceived shared values with and integrity of the hacktivists as most consistently emerging as important predictors of support for and resistance to hacktivism. Related to the targets, results indicated perceived competence and integrity of targets may be more important for reducing support for hacktivism and perceived benevolence of targets may be more important for increasing resistance.

Finally, relevant to Hypothesis 4, Table 2 indicates that participants' perceptions of utilitarian motives tended to be predictive of both support and resistance, as expected. Contrary to our

Table 2. Comparison of Patterns of Results From Hierarchical Multiple Regression Analyses.

Scenario	Dependent Variable			
Climategate	Cognitive/Affective Support	Behavioral Support	Cognitive/Affective Resistance	Behavioral Resistance
Step 1: General attitudes	(+) Admiration* (37%)	(+) Admiration* (22%)	(−) Admiration* (38%) **(+) Will report***	(−) Admiration* (50%) **(+) Will report***
Step 2: Attributions	**(+) Utilitarian*** (21%)	(+) Utilitarian* (5%)	(−) Utilitarian* (7%) (0) *Retributive*	(0) *Utilitarian* (2%)
Step 3: Trust/ distrust target (t)	**(−) Integrity (t)** (<1%)	**(−) Competence (t)*** (9%)		**(+) Benevolence (t)*** (4%)
Step 4: Trust/ distrust hacker (h)	**(+) Shared val, (h)***(21%) **(+) Unspec. trust (h)*** **(+) Integrity (h)***	**(+) Shared val. (h)*** (14%) **(+) Unspec. trust (h)***	(0) *Shared val. (h)* (8%) **(−) Unspec. trust (h)***	**(−) Shared val. (h)*** (4%)
Other scenarios	Cognitive/affective support	Behavioral support	Cognitive/affective resistance	Behavioral resistance
Step 1: General attitudes	(+) Admiration* (12%)	**(+) Admiration*** (26%)	(+) Will report* (17%)	**(+) Will report*** (38%)
Step 2: Specific scenario	(0) Scenarios* (10%)	(0) *Scenarios* (2%)	(0) *Scenarios* (1%)	(0) *Scenarios* (1%)
Step 3: Attributions	**(+) Utilitarian*** (49%) **(+) Retributive***	**(+) Utilitarian*** (35%) (+) Retributive*	**(−) Utilitarian*** (26%) (0) *Retributive*	(−) Utilitarian* (12%)
Step 4: Trust/ distrust target (t)	(0) *Competence (t)* (<1%) (0) *Integrity (t)*	**(−) Competence (t)*** (1%)	**(+) Benevolence (t)*** (4%)	**(+) Benevolence (t)*** (5%) (0) *Shared value (t)*
Step 5: Trust/ distrust hacker (h)	**(+) Shared value (h)*** (13%) **(+) Integrity (h)*** **(+) Benevolence (h)***	(0) *Shared value. (h)* (5%) **(+) Integrity (h)***	(0) *Shared value (h)* (16%) **(−) Integrity (h)*** **(+) No care impact (h)***	**(−) Shared value (h)*** (14%) **(+) No care impact (h)*** **(−) Benevolence (h)***

hypotheses, however, perceptions of retributive motives did not reliably relate to support and resistance and when they were predictive, they tended to predict more support and less resistance.

Mediation by Situation-Specific Perceptions

Relevant to RQ2, regarding mediation of the effects of attitudes by situation perceptions (illustrated by Figure 1), the hierarchical regression analyses summarized in Table 2 were suggestive: Although admiration was always a significant predictor when entered in Step 1 of the analyses, in all but one analysis it ceased to be predictive once all situation perceptions were entered. On the other hand, when willingness to report was a significant predictor, it tended to remain a significant predictor of resistance variables, even in the full models.

To more formally explore the possibility of mediation, we conducted additional analyses based on requirements for mediation (Baron & Kenny, 1986; Preacher & Hayes, 2008). Because of our small sample size, we used the bootstrapping macro recommended by Hayes (2013) to estimate the indirect effects. The results for cognitive/affective and behavioral support (and likewise for the resistance variables) were similar. Consequently, we used overall average of all support items as our dependent variable for support and the overall average of all resistance items as our dependent variable for resistance. When predicting support or resistance in the climategate or other scenarios, we tested the ability of all potentially important predictors listed in Table 2 for their ability to mediate the impacts of the general attitudes (admiration in the case of support, and willingness to report in the case of resistance) on the dependent variables.

As shown in Table 3, the effects of admiration on support for hacktivism were significantly mediated by situation-specific perceptions in the results from the climategate scenario and from the other scenarios. Also, the effect of willingness to report hacktivism on resistance to hacktivism was significantly mediated by situation-specific perceptions in the analysis of other scenarios. However, mediation of attitude's effect on resistance did not achieve significance in analysis of the climategate scenario.

Across all analyses, it appeared that perceptions of shared values with and integrity of the hacktivist were the most important mediators (consistent with results in Table 2). However, the individual variables identified as significant mediators varied across analyses, suggesting the importance of certain mediators may vary dependent on other situation-specific factors.

Discussion

The purpose of this study was to explore the predictors of support for and resistance to hacktivism among onlookers who, in this case, were STEM students early in their college careers. Early career students are especially apt subjects because it is likely that future hacktivists would come from this population (Yar, 2005). For our predictors, we focused on proximate psychological factors: general attitudes toward hacktivism and specific situation perceptions. Thus, our approach is distinctly psychological and focuses on the individual, in the same spirit as prior research on engagement in social protests, which has focused on the role of factors such as social identity, efficacy, relative deprivation, and so on (e.g., Brunsting & Postmes, 2002; Kelly & Kelly, 1994).

Because "distrust" is a commonly cited characteristic of hacktivists, we diverged from prior literature on social protest by focusing especially on the onlooker assessments of trustworthiness, of both the hacktivist attackers, and their targets. Although social protest research commonly assesses trust in government generally (calling it "external efficacy") (Van Stekelenburg & Klandermans, 2013), ours is the first article to our knowledge that focuses on both trust in the targets and trust in initiators of social protest and also focuses on specific trustworthiness perceptions instead of trust in general. Within the literature on hacktivism as a specific form of protest, it is also the first (again, to our knowledge) to analyze why onlookers might support or resist such attacks.

Table 3. Mediation of Attitude Variables by Perception Variables, for Predicting Support and Resistance.

	IV to Mediator		Mediator to DV		Indirect Effect PE		Indirect Effect CI	
Mediators	*A*	(*SE*)	*B*	(*SE*)	A × B	(*SE*)	Lower	Upper
Climategate								
Support (DV)	C = .490***	(.079)	C’ = .102	(.080)	Total = .390$^\wedge$	(.096)	.213	.597
Admire (IV)								
Utilitarian	.562***	(.097)	.108	(.105)	.062	(.066)	−.076	.187
Retribution	.452***	(.096)	−.019	(.100)	−.004	(.051)	−.110	.089
Integrity (t)	−.054	(.107)	−.021	(.075)	.001	(.012)	−.014	.042
Comp. (t)	−.122	(.087)	−.139	(.092)	.021	(.024)	−.005	.102
Unspec. (h)	.392***	(.084)	.290*	(.126)	.104	(.074)	−.017	.274
Sh. Val. (h)	.441***	(.075)	.333**	(.103)	.140$^\wedge$	(.069)	.034	.317
Integrity (h)	.402***	(.075)	.130	(.127)	.059	(.070)	−.095	.182
Benevol. (h)	.252**	(.085)	.021	(.098)	.008	(.032)	−.068	.064
Resist (DV)	C = .508***	(.063)	C’ = .421***	(.055)	Total = .090	(.060)	−.020	.214
Will report (IV)								
Utilitarian	−.226*	(.105)	−.078	(.094)	.020	(.029)	−.020	.097
Retribution	−.120	(.091)	.093	(.093)	−.010	(.017)	−.072	.008
Benevol. (t)	−.004	(.076)	.125	(.110)	−.002	(.015)	−.037	.027
Sh. Val. (t)	−.081	(.098)	.051	(.085)	−.004	(.014)	−.069	.009
Unspec. (h)	−.213*	(.085)	.021	(.125)	−.002	(.033)	−.071	.067
Sh. Val. (h)	−.167*	(.082)	−.181^{+}	(.095)	.030	(.024)	−.001	.106
Integrity (h)	−.194*	(.079)	−.188	(.116)	.035	(.031)	−.004	.128
Benevol. (h)	−.060	(.084)	−.228*	(.091)	.016	(.033)	−.031	.116
No care (h)	.239^{+}	(.122)	.039	(.052)	.009	(.016)	−.014	.058

(continued)

Table 3. (continued)

	IV to Mediator		Mediator to DV		Indirect Effect PE		Indirect Effect CI	
Mediators	*A*	(*SE*)	*B*	(*SE*)	A × B	(*SE*)	Lower	Upper
Other scenarios								
Support (DV)	C = .474***	(.108)	C' = .139*	(.060)	Total = .346^	(.124)	.089	.576
Admire (IV)								
Utilitarian	.376**	(.118)	.352***	(.070)	.139^	(.055)	.045	.264
Retribution	.357**	(.127)	.166*	(.077)	.056^	(.040)	.004	.180
Integrity (t)	.054	(.138)	−.006	(.062)	−.001	(.009)	−.022	.017
Comp. (t)	.029	(.139)	−.126*	(.054)	−.003	(.023)	−.058	.036
Unspec. (h)	.424***	(.094)	−.049	(.122)	−.020	(.064)	−.172	.090
Sh. Val. (h)	.356**	(.107)	.148$^+$	(.078)	.059	(.043)	−.011	.152
Integrity (h)	.327**	(.098)	.282*	(.122)	.093^	(.059)	.006	.243
Benevol. (h)	.149	(.109)	.159*	(.075)	.021	(.024)	−.008	.105
Resist (DV)	C = .553***	(.094)	C' = .277***	(.077)	Total = .278^	(.115)	.024	.489
Will report (IV)								
Utilitarian	−.257*	(.113)	−.098	(.091)	.029	(.037)	−.028	.123
Retribution	−.282*	(.120)	−.094	(.096)	.027	(.040)	−.021	.158
Benevol. (t)	.116	(.120)	.211$^+$	(.112)	.023	(.034)	−.010	.147
Sh. Val. (t)	−.132	(.122)	−.076	(.094)	.009	(.026)	−.019	.093
Unspec. (h)	−.450***	(.084)	.149	(.155)	−.055	(.087)	−.234	.105
Sh. Val. (h)	−.347***	(.099)	−.234*	(.100)	.084^	(.056)	.002	.227
Integrity (h)	−.371***	(.088)	−.193	(.154)	.062	(.079)	−.076	.240
Benevol. (h)	−.169+	(.100)	−.283**	(.093)	.045	(.032)	−.000	.141
No care (h)	.267*	(.131)	.211***	(.056)	.053^	(.036)	.003	.152

Note. A = path A from the independent variable (IV) of admiration for hacktivists (admire) or willingness to report hacktivism (will report) to the individual mediators; B = path B from the individual listed mediators to the dependent variable (DV) of support for hacktivism (support) or resistance to hacktivism (resist); A × B = bootstrap point estimates of indirect effects using Preacher and Hayes (2008) INDIRECT macro for SPSS. PE = point estimates for indirect effects; CI = bias corrected 95% confidence intervals for indirect effects estimated using bootstrapping procedures (1,000 bootstrap samples); C = path from the IV admire or will report to the respective DV support or resist with no mediators included in the model; C' = path from the IV admire or will report to the respective DV support or resist with all mediators included in the model. Variable abbreviations: (t) = variable pertains to trust in target; (h) = it pertains to trust in hacktivist; Comp. = competence; Unspec. = unspecified trust; Sh. Val. = Shared values; Benevol. = benevolence.

$^+p < .10$. $^*p < .05$. $^{**}p < .01$. $^{***}p < .001$. ^Significant $p < .05$ indirect effect based on bootstrapped point estimates and confidence intervals.

The lack of prior research created a challenge in selecting the measures to assess our constructs. We thus created the measures we used. Because this is the first time our scales were used, our results are necessarily exploratory and tentative. Nonetheless, our item and scale analyses and scenario comparisons provide preliminary evidence that the scales and subscales constructed for this investigation have adequate internal validity and are useful for detecting variations in hacktivism support/resistance, trustworthiness of hackers and targets, and attributions about the motivations of hacktivists.

For our exploration, we posited a number of hypotheses, illustrated by Figure 1. Regarding Hypothesis 1, preexisting global attitudes were predictive of hacktivism support and resistance in the specific scenarios. Given that the general attitude measures, to some extent, paralleled the measures of specific support and resistance (e.g., asking about willingness to report hacktivism generally and then asking about willingness to report it in a specific situation), this is not too surprising. Nonetheless, Hypothesis 1 was important to establish empirically because relationships between global and specific attitudes are not always straightforward (Gau, 2013). For example, somewhat surprisingly, general cognitive moral judgments of hacktivism were *not* as predictively useful as admiration and willingness to report, even though we did notice that written responses and the discussion frequently referred to whether or not participants felt hacktivist actions were moral, as exemplified by this quote: "There are certain things that you need to think about. You need to think about moral rights and legally. Morally, I think they did do the right thing because those people [the rape bystanders] should have been caught in trouble."

Our findings may suggest that, while general admiration and willingness to report hacktivism are relatively stable and useful predictors of people's support/resistance in specific situations, moral convictions about hacktivism may be more situation specific and affected by what and why specific hacktivist acts are undertaken. On the other hand, it is also possible that the highly cognitive nature of the study tasks affected the pattern of responses in this study. That is, admiration, moral judgment, and reporting refer, respectively, to one's affect, cognitive judgment, and behavior. The primary task in this study was highly cognitive—students read and made judgments about scenarios. The scenarios were not designed specifically to evoke emotion, nor did they require a behavioral response. However, by evoking specific judgments, the scenarios may have created a sort of "situation press" that reduced free expression of moral judgments and reduced the predictive ability of that dimension, as has been found in personality research (e.g., Tett & Guterman, 2000).

Consistent with our next two hypotheses, we also found trust and distrust in the targets (Hypothesis 2) and the hacktivists (Hypothesis 3) predicted willingness to support and resist hacktivism and accounted for significant variance in addition to global attitudes. However, examination of the variance accounted for suggested that our respondents were particularly attentive to whether or not they trusted the *hacktivists* as opposed to whether or not they trusted the targets when making their decisions about support or resistance in the specific situations. This is in spite of the fact that our scenarios created more between scenario variation in target trustworthiness than hacktivist trustworthiness (see Table 1). We had not specifically hypothesized this. To the contrary, drawing from prior writings on hacktivism, our investigation was inspired by the observation that lack of trust in the *targets* (who are often authorities or institutions) was professed as a major motivation of hacktivists.

A potential explanation for this finding is suggested by other results. Regarding Research Question 1, examination of the facets of trust that were revealed as most important by the hierarchical regression and mediation analyses suggested that respondents were especially attentive to whether or not they felt they shared values with the hacktivist, and whether they judged the hacktivists as high in integrity. This finding is consistent with social identity theory and other research finding that identifying with a group (e.g., in terms of sharing its values) predicts willingness to engage in group protest activities. Thus, for onlookers, it may be that social identity is a more powerful predictor than variables that describe grievances and relative deprivation (Van Stekelenburg & Klandermans, 2013). On the other hand, the cognitive processes may have been quite different if participants had been asked to judge the justifiability of hacktivism in a situation where they themselves were already established as the hacktivists. In such a case, self-perception biases (e.g., Bradley, 1978) may have allowed participants to assume their own trustworthiness and focus more upon the trustworthiness of the target.

We also found judgments of hacktivists' benevolence were sometimes predictive, but the competence of the hacktivists was not predictive of support and resistance. These findings are consistent with other research finding that judgments of moral dimensions of trustworthiness are often more numerous and have greater influences on trust than competence judgments (e.g., Krot & Lewicka, 2012; Landrum, Mills, & Johnston, 2013; Wasti, Tan, & Erdil, 2011). On the other hand, the facets of trust in the *target* that were most predictive did include competence (as well as benevolence and integrity) but did not usually include shared values.

This finding that the importance of facets may vary across situations is consistent with the findings for Research Question 2. Mediation tests of global attitudes by perceptions of the situation revealed three of the four tests of the indirect effects achieved significance. While the specific variables that had significant effects included shared values with and integrity of the hacktivists (providing further support for the importance of these variables), the significance of individual predictors varied across the four analyses. Future research attempting to better understand the mechanisms underlying support and resistance, for hacktivist or other social protest activities, may thus find it fruitful to study the conditions under which onlookers are affected most by different facets of trustworthiness.

Finally, perceptions of the utilitarian and retributive value of the hacktivism also predicted support and resistance. If hacktivism was perceived as usefully achieving some aim (e.g., revealing the truth, preventing harm), then it was more supported and less resisted. Less reliably, hacktivism perceived as more retributive (punishing the target), also predicted more support, in conflict with Hypothesis 4. Prior research has suggested that people will prefer retributive punishments under some conditions. For example, Carlsmith and Darley (2008) note, when faced with blameworthy harmful behaviors, through both intuition and perhaps motivated reasoning, the majority of people prefer to reciprocate with retributive punishments that would give others "what they deserve" rather than merely utilitarian punishments which might simply remedy damage or prevent future harm from occurring. Thus, it is possible that, in our scenarios, those who perceived the hacktivism as retributive also perceived the targets as blameworthy. Future research is needed, however, to clarify this point and examine the factors that moderate the impact of perceptions of retribution on support for or resistance to hacktivism.

Conclusions, Limitations, and Directions for Future Research

In conclusion, the present study advances the understanding of reasons why onlookers may support or resist hacktivist attempts. Global attitudes do appear to impact situation perceptions, especially perceptions of shared values with and the integrity of the hacktivists, and impact onlooker support and resistance. However, the present study was only a first exploration of our model, using new measures within a single convenience sample of STEM students. The measures show promising reliability and validity but should be tested in additional studies. Also, while it is useful to know what STEM students think—as they are most likely to be the technology-savvy leaders in the future—the present results may not generalize to all such STEM students or to other noncollege student populations. Future research should seek to replicate these findings, if possible in representative samples and nonclassroom settings. Also, to enhance external validity, we used four real-world descriptions of actual hacktivism situations as stimuli. Clearly, four scenarios cannot capture the full variation of possible hacktivist attacks, our results are likely affected by the specific scenarios chosen, and future research should include additional variants of hacktivism. Because this was a first exploration, we also did not seek to experimentally vary some of the variables that emerged as key predictors in the present study. Thus, our results are largely correlational findings and not adequate for establishing causality. Future research should thus focus on explicit experimental manipulations of factors such as perceived values, integrity, benevolence, and competence of hacktivists and their targets, in order to more firmly establish the causal relationships between these variables and support and resistance to hacktivism.

Authors' Note

We thank L. Dee Miller for his comments and suggestions and extend our appreciation to the students who offered their opinions and allowed us to analyze their responses to the scenarios.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported by a grant from the National Science Foundation (NSF-SBES-SATC-1228937). Opinions expressed in this report are solely those of the authors and not of NSF or other organization.

Notes

1. All appendices are available at http://go.unl.edu/sscr_pytlikzillig_2014 or from the first author.
2. Due to space constraints, illustrative items and ranges of Cronbach's αs are reported. The full set of items and specific reliability estimates for each scenario are available in online Appendix C at http://go.unl.edu/sscr_pytlikzillig_2014.
3. The understanding items had been included to assess cognitive/affective support and resistance but reduced the internal reliability of those subscales and therefore were not included in those subscales.
4. We conducted analyses both ways because, in the simultaneous regressions, the significant correlations among the predictors could result in the nonsignificance of individual predictors that would be significant if the other variables were not included in the model.
5. For those wishing to see the parameter estimates, they are available in online Appendix D at http://go.unl.edu/sscr_pytlikzillig_2014.

Supplementary Materials

The online appendices are available at http://ssc.sagepub.com/supplemental.

References

Ajzen, I. (1991). The theory of planned behavior. *Behavior and Human Decision Processes*, *50*, 179–211.

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, *52*, 27–58.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*, 1173–1182.

Bohner, G., & Dickel, N. (2011). Attitudes and attitude change. *Annual Review of Psychology*, *62*, 391–417.

Bradley, G. W. (1978). Self-serving biases in the attribution process: A reexamination of the fact or fiction question. *Journal of Personality and Social Psychology*, *36*, 56.

Brunsting, S., & Postmes, T. (2002). Social movement participation in the digital age predicting offline and online collective action. *Small Group Research*, *33*, 525–554.

Carlsmith, K. M., & Darley, J. M. (2008). Psychological aspects of retributive justice. *Advances in Experimental Social Psychology*, *40*, 193–236.

Corr, P. J. (2013). Approach and avoidance behaviour: Multiple systems and their interactions. *Emotion Review*, *5*, 285–290.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Pittsburgh, PA: RAND.

Feshbach, S. (1970). Aggression. In P. H. Mussen (Ed.), *Carmichael's manual of child psychology* (pp. 159–259). New York, NY: John Wiley.

Fleeson, W. (2007). Situation-based contingencies underlying trait-content manifestation in behavior. *Journal of Personality*, *75*, 825–861.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *Technology and Society Magazine, IEEE*, *30*, 28–38.

Gau, J. M. (2013). Procedural justice and police legitimacy: A test of measurement and structure. *American Journal of Criminal Justice*, *39*, 187–205. doi:10.1007/s12103-013-9220-8.

Gray, J. A. (1991). Neural systems, emotion and personality. In J. Madden (Ed.), *Neurobiology of learning, emotion, and affect* (Vol. 4, pp. 273–306). New York, NY: Raven.

Hamm, J. A., PytlikZillig, L., Herian, M. N., Bornstein, B. H., Tomkins, A. J., & Hoffman, L. (2013). Deconstructing public confidence in state courts. *Journal of Trust Research*, *3*, 11–31.

Hareli, S., & Weiner, B. (2002). Social emotions and personality inferences: A scaffold for a new direction in the study of achievement motivation. *Educational Psychologist*, *37*, 183–193.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Press.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*, 20–40.

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure online and offline. *Crime & Delinquency*, *58*, 798–822.

Jordan, T., & Taylor, P. A. (2004). *Hacktivism: Rebels with a cause*. London, England: Routledge.

Kanekar, S., Bulsara, R. M., Duarte, N. T., & Kolsawalla, M. B. (1981). Perception of an aggressor and his victim as a function of friendship and retaliation. *The Journal of Social Psychology*, *113*, 241–246.

Kelly, C., & Kelly, J. (1994). Who gets involved in collective action?: Social psychological determinants of individual participation in trade unions. *Human Relations*, *47*, 63–88.

Krot, K., & Lewicka, D. (2012). The importance of trust in manager-employee relationships. *International Journal of Electronic Business Management*, *10*, 224–233.

Landrum, A. R., Mills, C. M., & Johnston, A. M. (2013). When do children trust the expert? Benevolence information influences children's trust more than expertise. *Developmental Science*, *16*, 622–638.

Levy, S. (2001). *Hackers: Heroes of the computer revolution* (Vol. 4). New York, NY: Penguin Books.

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: Toward a hacktivist ethic. *ACM SIGCAS Computers and Society*, *30*, 14–19.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*, 709–734.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, *40*, 879–891.

PytlikZillig, L. M., Tomkins, A. J., Herian, M. N., Hamm, J. A., & Abdel-Monem, T. (2012). Public input methods and confidence in government. *Transforming Government: People, Process and Policy*, *6*, 92–111.

Samuel, A. W. (2004). *Hacktivism and the future of political participation*. (Dissertation), Harvard University Cambridge, Massachusetts. Retrieved from http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-frontmatter.pdf

Schussman, A., & Soule, S. A. (2005). Process and protest: Accounting for individual protest participation. *Social Forces*, *84*, 1083–1108.

Siegrist, M., Cvetkovich, G., & Roth, C. (2000). Salient value similarity, social trust, and risk/benefit perception. *Risk Analysis*, *20*, 353–362.

Taylor, P. A. (2005). From hackers to hacktivists: speed bumps on the global superhighway? *New Media & Society*, *7*, 625–646.

Tett, R. P., & Guterman, H. A. (2000). Situation trait relevance, trait expression, and cross-situational consistency: Testing a principle of trait activation. *Journal of Research in Personality*, *34*, 397–423.

Van Stekelenburg, J., & Klandermans, B. (2013). The social psychology of protest. *Current Sociology*, *61*, 886–905.

Warren, M. J. (2008). Hackers and cyber terrorists. In M. Quigley (Ed.), *Encyclopedia of information ethics and security* (pp. 304–311). Hershey, PA: IGI Global.

Wasti, S. A., Tan, H. H., & Erdil, S. E. (2011). Antecedents of trust across foci: A comparative study of Turkey and China. *Management and Organization Review*, *7*, 279–302.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review*, *92*, 548–573.

Weiner, B. (2010). The development of an attribution-based theory of motivation: A history of ideas. *Educational Psychologist*, *45*, 28–36.

Workman, M., Phelps, D. C., & Hare, R. C. (2013). A study of performative hactivist subcultures and threats to businesses. *Information Security Journal: A Global Perspective*, *22*, 187–200.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*, 64–74.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*, 387–399.

Author Biographies

Lisa M. PytlikZillig is a social psychologist and research associate professor at the University of Nebraska Public Policy Center. Her research especially focuses on trust in institutions and processes for enhancing effective public engagement in policy discussions. E-mail: lpytlikz@nebraska.edu.

Shiyuan Wang is a graduate research assistant at Public Policy Center and a doctoral student at Educational Psychology Department, University of Nebraska–Lincoln. Her research at the center focuses on the influences of trust, attitudes, and motives in hacktivism. E-mail: wang.shiyuan@huskers.unl.edu.

Leen-Kiat Soh is an associate professor in the Department of Computer Science and Engineering at the University of Nebraska, Lincoln, NE. His research interests include multiagent system areas such as team formation, multiagent learning, resource-aware sensing, with applications in computer-supported collaborative learning, survey informatics, intelligent user interfaces, and agent-based modeling and simulations. E-mail: lksoh@cse.unl.edu.

Alan J. Tomkins is a professor in the University of Nebraska–Lincoln's Law/Psychology Program and since 1998 has served as director of the University of Nebraska Public Policy Center. His research interests currently focus on trust (and distrust) in governmental institutions and the public's effective and meaningful participation in policy decision making. E-mail: atomkins@nebraska.edu.

Ashok Samal is a professor of computer science and engineering at the University of Nebraska–Lincoln. His research interests include data mining and image analysis. E-mail: samal@cse.unl.edu.

Tonya K. Bernadt is the education and outreach specialist for the National Drought Mitigation Center at University of Nebraska–Lincoln. Her primary work includes stakeholder engagement, facilitation, developing education programs, and working on various research grants. E-mail: tbernadt5@unl.edu.

Michael J. Hayes is a professor in the applied climate science area within the School of Natural Resources and the Director of the National Drought Mitigation Center (NDMC) located at the University of Nebraska. E-mail: mhayes2@unl.edu.