Article

Examining Willingness to Attack Critical Infrastructure Online and Offline

Crime & Delinquency
58(5) 798–822

DOI: 10.1177/0011128712452963
http://cad.sagepub.com
SAGE

Thomas J. Holt[1] and Max Kilger[2]

Abstract

The continuing adoption of technologies by the general public coupled with the expanding reliance of critical infrastructures connected through the Internet has created unique opportunities for attacks by civilians and nation-states alike. Although governments are increasingly focusing on policies to deter nation-state level attacks, it is unclear what factors may affect citizens' decisions to engage in politically motivated cyber crime attacks against either a foreign nation-state or their own homeland. Thus, this study will explore the factors that may affect individual willingness to use technology to attack critical infrastructure online or offline using an international sample of college students. The findings compare the correlates of physical and virtual attacks, including political outlook, group equality, and involvement in cyber deviance. The implications of this research on the relationship between on- and offline infrastructure attacks will be explored in depth for policy makers, governmental agencies, and law enforcement.

Keywords

cyberterror, critical infrasctruture, hacking, cybercrime, extremism`

[1]Michigan State University, East Lansing, USA
[2]Spartan Devils Honeynet Chapter, East Lansing, MI, USA

Corresponding Author:
Thomas J. Holt, School of Criminal Justice Michigan State University 434 Baker Hall East Lansing, MI 48824
Email: holtt@msu.edu

The global adoption of technology over the last two decades has radically altered the way individuals, businesses, and governments communicate. Access to high-speed wireless connectivity coupled with the increased use of mobile computers and smart phones enables individuals to be in constant contact with others in near-real time through forms of computer-mediated communications (CMCs), such as email, text messaging, and Facebook. Governments, defense agencies, and financial institutions depend on technology to maintain large scale databases of information and intellectual property, as well as communicate directly with the general public (Brenner, 2008; Jennings & Zeitner, 2003; Van Laer, 2010). The proliferation of technology has also engendered the automation and management of critical infrastructure, including telephony, water, sewer, and power systems via remote computer systems (Brodscky & Radvanovsky, 2011; Kilger, 2011).

As a consequence, cyberspace and technological resources are a key target for politically motivated attacks and social conflict (Arquilla & Ronfeldt, 1998; Brenner, 2008; Denning, 2011; Holt, 2009). The Internet and CMCs provide individuals with an outlet to express dissent with policies and practices of their own government or those of foreign nations (DiMaggio, Hargittai, Neuman, & Robinson, 2001; Van Laer, 2010; Vasi, 2006). These technologies also allow nation-states' most vulnerable and critical systems to be attacked with greater secrecy and fewer resources than might otherwise be required offline (Brodscky & Radvanovsky, 2011; Wilson, 2008).

Policy makers have increasingly focused on deterring cyber attacks performed by state-sponsored actors (Brenner, 2008; U.S. Department of Defense, 2011), though there has been less focus placed on the role of actors with no ties or sponsorship from a nation or military group (Denning, 2011; Kilger, 2011). Non-nation-state-sponsored actors can leverage technological resources as a force multiplier to engage in nonviolent actions like protest, or serious forms of violence such as targeted attacks against infrastructure with a greater magnitude than what may otherwise be possible through real-world protest and political action (Brenner, 2008; Jordan & Taylor, 2004; Kilger, 2011). The faceless, borderless nature of the Internet also allows individuals to efficiently mask their real identity and reduce their likelihood of detection (Brenner, 2008; Denning, 2011). These conditions have given rise to the "civilian cyber warrior" who can operate with no state sponsorship to attack various resources within their own government or a foreign nation due to the power differential provided by the Internet and CMCs (Denning, 2011; Kilger, 2011).

Few researchers have considered what individual factors may predict participation as a cyber warrior against either their home country or another

nation. Furthermore, it is unclear what relationships may be evident in the predictors of nonviolent and violent activities in physical and virtual action. Attitudinal factors, such as national pride or belief in group equality, appear to influence violent political action in the real world, though it is unclear how they may affect the decision to engage in cyber attacks. This exploratory study will examine these issues using an international sample of college students from a Midwestern university. The findings provide initial insights into facto that predict individual willingness to act as a cyberwarrior, and consider the implication of these findings for policy makers, intelligence communities, and law enforcement.

Exploring the Relationship Between Political Action On- and Offline

The role of the Internet and CMCs in political action can be situated in the larger spectrum of political actions performed by non-nation-state actors (Schmid, 1988, 2004). There are myriad nonviolent acts of resistance that may be used, which do not violate legal statutes but instead express an opinion or belief, including letter writing and protests (Martin, 2006; Schmid, 1988, 2004). The most extreme forms of political action involve planned acts of violence, such as the use of explosive devices or assassinations in support of an ideology (Schmid, 2004). Such incidents may be defined as acts of terror, particularly if the targets are located within an actors' home country or designed to affect political and psychological effects on a domestic population (Martin, 2006; Schmid, 2004).[1] Some may define this behavior as an act of domestic terror, whereas attacks against foreign resources or installations to affect an international population or policies make it an act of international terror (Martin, 2006; Schmid, 2004).

The substantive harm to people and property that may result from a physical terror attack are largely absent in most cyber attacks to date (Brenner, 2008; Britz, 2010). Physical destruction is not, however, necessary in online environments as attackers can target the electronic infrastructure that undergird financial institutions or power systems to produce a loss of service (Brenner, 2008; Britz, 2010; Brodscky & Radvanovsky, 2011; Denning, 2011). The resulting economic harm or disruption of services produced, combined with concerns over the likelihood that such an attack could be repeated, may equal that of a physical terror attack. As a result, the use of destructive attacks against critical infrastructure online may be just as harmful as those designed to affect targets in the real world (Britz, 2010; Denning, 2011; Kilger, 2011).

The wide range of political action that people may engage in across virtual and real environments makes it difficult to identify consistent predictors for participation (Schussman & Soule, 2005). There is a substantive body of research on participation in nonviolent political action in the real world (Huddy & Khatib, 2007; Pettigrew, 2003; Schussman & Soule, 2005), though few focus on cyber activism (Al-Rizzo, 2008; Holt, 2009; Stepanova, 2011; Vasi, 2006). One reason for the limited body of scholarship is the lack of data on participation in extreme acts of violence. It is clear that the impact of an attack on property and human casualties appears to influence the overall participation rates for these attacks (Martin, 2006; Post, 1998). For instance, participation in nonviolent forms of political action such as protest are increasingly common (Putnam, 2000), though fewer individuals engage in extreme forms of violence, including bombings and personal violence (Martin, 2006). Similarly, the frequency with which individuals engage in serious attacks against critical infrastructure via the Internet is thought to be relatively low given its overall prevalence across the globe (Brenner, 2008; Denning, 2011).

As a consequence, it is not clear what factors may drive individual willingness to engage in violent political action online, and what similarities may exist across virtual and real environments. Research on the range of real-world acts of violent and nonviolent action suggests there may be several attitudinal factors that may influence behavior. Specifically, the concept of patriotism may affect violence, operationalized as the degree of pride in and love for one's nation (Brewer, 1999; Kosterman & Feshbach, 1989). Individuals with a substantial emotional attachment toward their homeland may be unwilling to take political action against it or damage its reputation (Brewer, 1999; Schatz, Staub, & Lavine, 1999). The significance of patriotism is, however, mixed in the research literature making it difficult to fully discern the role that patriotism may play in political action (Huddy & Khatib, 2007; Schatz et al., 1999).

In much the same way, individual acceptance of nationalism may affect attitudes toward protest and political violence. Nationalism is highly related to patriotism, though this construct largely focuses on perception that a person's home country is better than others, and should be a dominant force globally (Kosterman & Feshbach, 1989; Schatz et al., 1999). Those who report a high degree of nationalism and patriotism may be more inclined to engage in attacks on foreign governments (Duckitt, 2003; Herrmann, Tetlock, & Visser, 1999; Huddy & Khatib, 2007; Van Evera, 1994). Individuals with minimal nationalistic attitudes may also be inclined to engage in political actions against their home country because they do not agree with its policies or

stances (Conover, Searing, & Crewe, 2004; Terry, Hogg, & Duck, 1999). It is not clear how nationalism may influence online behaviors (see Van Laer, 2010), making it difficult to identify what role nationalism may play in Internet-based actions against foreign and domestic targets.

Individual attitudes toward equality and minority groups may also increase willingness to engage in political activity (Vollhardt, Migacheva, & Tropp, 2009). Specifically, a strong belief in group equality may lead some to take action in support of a general collective identity that they feel is being ignored or marginalized (Friedkin, 2004; Vollhardt et al., 2009). Individuals may also engage in acts of terror or political action in the real world to maintain or achieve group solidarity (Post, 1998). Attitudes toward marginalized groups in society may actually serve as a disruptive force in societies, whether for domestic or international relationships (Kunovich & Hodson, 1999; Pettigrew, 2003; Vollhardt et al., 2009). The identification of an out-group can be used as a rallying point for social cohesion in support of violence or political action, especially against foreign entities. In addition, those with less tolerance for out-groups may be less tolerant of different opinions and dissent from social norms (Kunovich & Hodson, 1999; Mummendey, Klink, & Brown, 2001). Support for groups that are held down or otherwise socially isolated may also increase some individuals' willingness to engage in political activity to ensure that they receive equal treatment by the larger group (Lavis & Stoddard, 2003).

The unique technological aspects of cyberspace may present a barrier to individuals interested in engaging in violence against virtual targets, though it is unclear how it might affect willingness to engage in real-world activities. For instance, the hacker community has long supported left-leaning ideals that information should be free and that government and industry stymie creativity and may not be worthy of trust (Holt, 2007; Levy, 2001). Although hackers frequently attack targets for monetary gain (Chu, Holt, & Ahn, 2010; Kilger, 2011), an increasing number target government and industry resources based on individual political, nationalistic, and religious motives (Al-Rizzo, 2008; Holt, 2009; Kilger, 2011). In fact, web defacements by politically motivated hacker groups are common following political events in the real world (Al-Rizzo, 2008; Denning, 2011; Kilger, 2011; Woo, Kim, & Dominick, 2004).

At the same time, technological skill may have little predictive capability because individuals need not have significant knowledge of technology to engage in some forms of online activity. Tutorials and tools are often freely available and used as a means to encourage unskilled actors to engage in attacks against various targets (Chu et al., 2010; Denning, 2011; Holt, 2009;

Jordan & Taylor, 2004). Hacker groups and political attackers have distributed such resources over the last two decades to draw in interested parties to assist in attacks (Denning, 2011; Jordan & Taylor, 2004). Thus, technological skill may have a mixed effect on political action in virtual and real environments.

There may also be some tie between involvement in political actions in online environments and general participation in online deviance, particularly digital piracy. Those who engage in piracy tend to disregard copyright law and discredit the impact of their actions on private industry and governments (Higgins, 2005; Hinduja, 2001; Holt, Burruss, & Bossler, 2010). Individuals involved in the hacker group Anonymous have engaged in a series of attacks against private industry and governments around the world in protests against attempts to reduce media piracy (Correll, 2010; Poulsen, 2011). The group espouses that governments are stifling the free flow of information and media companies are unfairly restricting access to materials thereby requiring a response from frustrated citizens. This suggests that involvement in piracy may foster willingness to engage in political activity online, though it likely has no influence on real-world action.

Finally, there are some demographic characteristics that may predict participation in different forms of political violence on- and offline. For instance, an individual's country of origin appears to differentially affect willingness to engage in political protest on- and offline. Citizens of democracies may be more likely to engage in real-world protest as they have greater freedom to speak freely about their government (Huddy & Khatib, 2007; Schatz et al., 1999). Individuals from repressive regimes may find less risk in protest actions in online environments where their identity can be shielded (Stepanova, 2011). In addition, males are more likely to engage in protest activities (Dalton, 2002; Verba, Schlozman, & Brady, 1995) and more extreme forms of political violence (Martin, 2006; Putnam, 2000). Men also more frequently engage in hacking and cyber crime generally (Bossler & Burruss, 2011; Hinduja, 2001; Skinner & Fream, 1997). Younger people also tend to engage in protest activities in the real world (Wiltfang & McAdam, 1991) and various forms of deviance in online environments (Holt et al., 2010; Skinner & Fream, 1997). Thus, U.S. citizens, males, and younger people may be more likely to engage in political activities on- and offline.

The Present Study

Taken as a whole, there is some prospective linkage between politically motivated behaviors on- and offline, ranging from acts of nonviolent

resistance to extreme acts of violence against civilian and government targets. As a consequence, it is not clear what factors may drive individual willingness to engage in violent political action on- or offline and what similarities may exist across these environments. Furthermore, it is unclear what relationships may be evident in the predictors of nonviolent and violent activities in physical and virtual action. Finally, it is unclear how the target of an act, whether foreign or domestic, affects willingness to engage in various physical and virtual political activities. This study provides an exploratory analysis of the factors that affect individual willingness to engage in extreme political action on- and offline against domestic and foreign targets.

Method

Data for this study were generated from a self-report survey administered to undergraduate and graduate students at a large Midwestern university in the spring of 2010 using an online survey instrument. Using Dillman's (2007) Tailored Design Method, an email solicitation was delivered to a 25% stratified sample of the undergraduate and graduate student population. Respondents received a link to an electronic survey instrument along with the ethical guidelines of the study. A total of 357 individuals responded to the survey, which is a low response rate (5% of all recipients) but consistent with the overall trend of declining survey response rates (Campos, Zucoloto, Bonafe, Jordani, & Maroco, 2011; Curtin, Presser, & Singer, 2005; Fan & Yan, 2010). The final sample size was 353 respondents due to missing data. The respondents were 60% male, which is slightly higher than the larger university composition (48% male) and closely represents the age distribution of the university (average age was 22 in both contexts). In addition, the proportion of domestic (89%) to international students (11%) reflects the general university composition as a whole.

Critics commonly question the utility of college samples due to their limited generalizability (see Oakes, 1972; Payne & Chappell, 2008). College students provide a pertinent sample population, however, for research on computer skill, early adoption of technology, and participation in cyber deviance though they are frequently used in criminological research as a whole (Bossler & Burruss, 2011; Higgins & Wilson, 2006; Hinduja, 2001; Holt et al., 2010; Skinner & Fream, 1997). In addition, young people are more likely to engage in protest activities (Wiltfang & McAdam, 1991) and are less likely to have "crystallized attitudes and less formulated senses of self" (Sears, 1986). Thus, college students are an appropriate population to explore the predictors for political action on- and offline.

Dependent Variables

To examine willingness to engage in the spectrum of politically motivated action on- and offline, respondents in the study were presented with scenarios involving nation-state actions causing harm to the citizens of their home country. The study design was a 2 × 2 factor design that involved the type of attack and the identity of the nation-state causing the harm. A scenario design was used due to the relatively limited proportion of individuals actively engaging in attacks against critical infrastructure on- and offline (Brenner, 2008; Britz, 2010). Scenarios have been used in a variety of criminological and political science research (Fishbein & Ajzen, 1975; Higgins, 2005; Nagin & Paternoster, 1993; Piquero & Bouffard, 2007). In fact, scenario-based measures of future behavior appear to be valid constructs for actual behavior (Fishbein & Ajzen, 1975; Kim & Hunter, 1993). Thus, utilizing a scenario-based measure is a reasonable data source to explore the phenomena of attacks against nation-states in cyberspace and the real world.

The first scenario presented to respondents required them to consider how they might react under the following conditions:

> Imagine that the country that *you* most closely associate as your home country or homeland has recently promoted national policies and taken physical actions that have had negative consequences to your country. These policies and actions have resulted in significant hardships for the people in your home country. What actions do you think would be appropriate for you to take against your home country given their policies and physical actions? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

Respondents were then asked to select as many physical actions they would take against their home country in response to the perceived injustice as they felt necessary from eight items: (a) do nothing—let your country correct its actions on its own, (b) write a letter to your home country's government protesting their actions, (c) participate in a protest against your home country at an antigovernment rally, (d) protest at your home country's capitol building, (e) confront one of your home country's senior government official about his or her policies, (f) sneak into a military base in your home country to write slogans on buildings and vehicles, (g) physically damage an electrical power substation in your home country, and (h) damage a government building in your home country with an explosive device.

In addition to physical activities, respondents were also asked the following:

> What online activities do you think would be appropriate for you to take against your home country given their policies and physical actions? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

The respondent was presented with nine actions to perform in a cyber environment: (a) do nothing—let your country correct its actions on its own, (b) post a comment on a social networking website like Facebook or Twitter that criticizes your home country's government, (c) deface the personal website of an important government official for your home country, (d) deface an important official government website for your home country, (e) compromise the server of a bank in your home country and withdraw money to give to the victims of the government's policies and actions, (f) search your home country's government servers for secret papers that you might be able to use to embarrass the government, (g) compromise one or more of your home country's military servers and make changes that might temporarily affect their military readiness, (h) compromise one of your home country's regional power grids which results in a temporary power blackout in parts of your home country, and (i) compromise a nuclear power plant system that results in a small release of radioactivity in your home country.

The same language was used to assess individual willingness to engage in actions against a foreign nation-state inflicting harm on his or her homeland. This scenario utilized the fictitious nation of Bagaria as the target of attacks to avoid prospective respondents' biases against either foreign nations or ethnic or racial groups. The following language was used in this Bagarian scenario:

> Imagine that the country of Bagaria has recently promoted national policies and taken physical actions that have had negative consequences to the country that *you* most closely associate as your home country or homeland. These policies and actions have also resulted in significant hardships for the people in your home country.
>
> What actions do you think would be appropriate for you to take against Bagaria given their policies and physical actions against your home country? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

The same response sets for both physical and cyber action were presented to the respondent with the phrase Bagaria used in place of home country in the wording of the questions to compare variations in action based on foreign or domestic targets.

Independent Variables

To assess the role that national identity or patriotism plays in their decision making, a factor score was created utilizing measures derived from Kosterman and Feshbach (1989). Specifically, respondents were asked to rate their agreement (1 = *strongly disagree*; 4 = *strongly agree*) with six items relating to their emotional connection to their home country: (a) I am proud to be a citizen of my home country; (b) in a sense, I am emotionally attached to my home country and am emotionally affected by its actions; (c) although at times I may not agree with the government, my commitment to my home country always remains strong; (d) I feel a great pride in the land that is my home country; (e) when I see my home country's flag flying, I feel great; and (f) the fact that I am a citizen of my home country is an important part of my identity. The responses to these six items were summed and provide a reliable scale ($\alpha = .901$) measuring emotional attachment to their home country (see Table 1 for details).

To consider the role of nationalism in the willingness to engage in attacks, a three-item scale was adapted from Kosterman and Feshbach (1989). These items assess the perception that their home country is superior to other nations and rate their agreement with the sentiment (1 = *strongly disagree*; 4 = *strongly agree*). These items specifically are as follows: (a) Other countries should try to make their government as much like my home country's government as possible; (b) generally, the more influence my home country has on other nations, the better off they are; and (c) foreign nations have done some very fine things, but my home country does things in the best way of all. The responses were summed to create a parsimonious scale ($\alpha = .835$) to assess respondents' support for nationalism.

Given the role of group equality as a predictor in protest activities (Vollhardt et al., 2009), a factor score was created using six items adapted from Sidanius and Pratto (2001). These measures include the following: (a) It would be good if groups could be equal, (b) group equality should be our ideal, (c) all groups should be given an equal chance in life, (d) we should do what we can to equalize conditions for different groups, (e) we would have fewer problems if we treated people more equally, (f) we should strive to make incomes as equal as possible, and (g) no group should dominate in society. Respondents were

Table 1. Sample Descriptives (n = 353)

Variables	*M*	*SD*	Minimum	Maximum
Physical actions homeland	2.22	1.51	1	7
Physical actions Bagaria	1.61	1.39	1	7
Cyber actions homeland	1.24	1.26	1	8
Cyber actions Bagaria	1.23	1.21	1	8
Patriotism	19.13	4.01	6	24
Nationalism	5.86	2.18	3	12
Group equality	18.89	3.99	6	24
Out-group antagonism	7.90	3.28	5	20
Technological skill	3.08	3.20	3	15
Piracy	1.67	2.25	0	8
Country of origin	0.10	0.30	0	1
Gender	0.60	0.49	0	1
Age	22.29	3.36	18	31

asked to rate their agreement with these statements (1 = *strongly disagree*; 4 = *strongly agree*) and all responses were summed to create a reliable scale (α = .880). These items have been used to assess racism and prejudice (Sibley, Robertson, & Wilson, 2006), and provide a practical metric to explore attitudes toward marginalized groups in society.

To assess out-group antagonism, five measures were adapted from Sidanius and Pratto (2001): (a) Some groups of people are simply inferior to other groups; (b) if certain groups stayed in their place, we would have fewer problems; (c) it is probably a good thing that certain groups are at the top and other groups are at the bottom; (d) inferior groups should stay in their place; and (e) sometimes other groups must be kept in their place. Responses to each of these items (1 = *strongly disagree*; 4 = *strongly agree*) were summed (α = .866) to create a single-scaled item.

To examine the relationship between political and social activism in on- and offline environments, an additive scale was created to consider the range of physical and cyber actions an individual was willing to perform against either their home country or Bagaria. This scale was created by combining the binary measure for each of the seven physical action options together for both the homeland (α = .674) and Bagarian (α = .632) scenarios. The same process was performed for each of the eight cyber measures (homeland α = .712; Bagaria = .657). The "do nothing" item was excluded to assess active

rather than passive forms of resistance and action. These scales are included in each analysis to identify the influence of willingness to engage in multiple cyber attacks on physical action and vice versa across domestic and foreign targeting.

A number of researchers have linked different types of hackers and their associated behaviors with different levels of technical skill (Bossler & Burruss, 2011; Holt, 2007). To assess familiarity with technological skills, three measures were included exploring their comfort with specific activities including the following: (a) using an operating system like Unix or Linux; (b) using a standard computer programming or scripting language like C++, Perl, or Java; and (c) installing an operating system like Unix or Linux. Responses ranged from 1 (*not at all comfortable*) to 5 (*very comfortable*), and provided a concise scale ($\alpha = .856$) indicating their overall exposure to more technical computing skills.

To assess involvement in cyber crime, respondents were asked how often they had performed two forms of piracy over the last 12 months: (a) knowingly use, make, or give another person a "pirated" copy of commercially sold computer software and (b) knowingly use, make, or give to another person "pirated" media (music, television show, or movie (Holt et al., 2010; Skinner & Fream, 1997). Responses ranged from 0 (*never*) to 4 (*1-2 times, 3-5 times, 6-9 times*, and *10 or more times*). These items were summed to assess frequency of participation in both forms of piracy ($\alpha = .656$).

Three demographic variables are included in these analyses based on the general literature on cyber crime and activism generally: country of origin, gender, and age. Country of origin is measured based on respondents' answers to the question what country they consider to be their homeland. The responses were converted into a binary measure for U.S. (0) and non-U.S. homeland respondents (1). Gender (*male* = 0; *female* = 1) is particularly significant in the prediction of cyber crime, as many hackers and individuals who engage in piracy tend to be male (Higgins, 2005; Holt et al., 2010; Skinner & Fream, 1997). Age is included to explore the relationship to political action in the real world (Wiltfang & McAdam, 1991) and cyberspace.

Findings

In examining the distribution of responses to each scenario question, it is apparent that most respondents are willing to engage in traditional forms of nonviolent political action in their home country and a foreign nation. For instance, 62% of respondents were willing to engage in protests in their home country, and 57% of respondents would protest Bagarian actions (see Table 2). Many also reported a willingness to write letters expressing their opinion

Table 2. Reported Willingness to Engage in Physical Actions

Response type	Homeland (*n* = 357)	Bagaria (*n* = 357)
Do nothing	116 (32.49%)	151 (42.30%)
Write a letter	248 (69.47%)	192 (53.78%)
Participate in a protest	223 (62.46%)	207 (57.98%)
Travel to protest at the capitol	194 (54.34%)	90 (25.21%)
Confront a government official	107 (29.97%)	68 (19.05%)
Sneak into a base	10 (2.80%)	7 (1.96%)
Damage a power substation	6 (1.68%)	8 (2.24%)
Damage with explosives	3 (0.84%)	2 (0.56%)

about the issues. A smaller proportion of respondents would engage in physical confrontations with political officials in the real world, though the response rates were somewhat similar between the homeland (29.97%) and Bagarian (19.05%) scenarios. Finally, almost all participants would not engage in physical attacks to critical infrastructure regardless of the target in keeping with generally limited participation in extreme acts of violence (Martin, 2006).

The distribution of responses in the virtual attack scenarios was somewhat similar to those for the real world, especially when they involve attacks against critical infrastructure (see Table 3). The most commonly reported act was posting messages on Facebook or social media in both the homeland (77.31%) and foreign scenarios (76.19%), respectively. This is sensible given the heavy use of this technology in the general public, as well as the critical role of social media in the recent social protests in the Arab Spring (Stepanova, 2011). Between 10% and 13% of all respondents were willing to perform web defacements, whether against Bagaria or their home country, respectively. Respondents were much less likely to engage in acts that directly affect critical infrastructure, including financial institutions and military servers. Finally, less than 3% of respondents were willing to target power grids (1.68% homeland; 3.08% Bagaria) and nuclear plants (0.84% homeland; 0.28% Bagaria). These figures suggest individuals are generally unwilling to engage in extreme violence, regardless of the target.

Regression Results

Regression models were created to explore the relationships between the various individual factors and the total number of activities individuals

would engage in on- and offline against their home country and Bagaria. The regression models for physical actions demonstrate differences in the predictors based on domestic or foreign targets (see Table 4). The models for physical attacks suggest that there was a positive relationship between the level of advanced technical computer skills (home $p = .027$; Bagaria $p = .046$) and willingness to engage in multiple forms of cyber attack in the home and foreign models (home $p < .001$; Bagaria $p < .001$). This is an especially interesting result in light of the number of counterterrorism experts who have focused upon the synergistic effects of a combined physical and cyber attack upon critical infrastructures (Wilson, 2008). In addition, two factors were significant in the homeland model which were not present in the Bagarian scenario. There was a negative relationship between support for antagonistic relationships toward minority groups and country of origin, suggesting that U.S. citizens may be more likely to engage in multiple attacks ($p = .001$).

Different relationships were evident in the models for cyber activities along with differences based on the target of attack (see Table 4). In the homeland model, there was a positive relationship between out-group antagonism and willingness to engage in multiple cyber attacks ($p = .009$). A positive relationship was also evident between country of origin and cyber attacks, suggesting that foreign citizens were more likely to take virtual actions against their homeland ($p = .026$). There were also two significant predictors across the home and Bagarian models: piracy and physical attacks. These relationships were positive and significant suggesting cyber attacks in general are influenced by participation in cyber crime and willingness to engage in multiple physical attacks. The absence of significant effects for nationalism and patriotism in both the cyber and physical attack scenarios provides no support for the notion that malicious actors are emboldened by political ideology.

Due to the variation in predictors noted in the previous models, additional binary logistic regression models were conducted for multiple forms of action across each physical and cyber-attack scenario to clarify what role individual factors may play in nonviolent and violent activity.[2] In examining the various forms of physical action across the homeland and Bagarian models, it is clear that there is a direct relationship between willingness to engage in attacks in a virtual environment and attacks in the real world (see Table 5). This is the only significant item across all models. There are, however, variations in the predictors for each form of attack. Those with greater levels of patriotism were more likely to write letters on behalf of their beliefs. Respondents with less support for out-group antagonism and U.S. residents were more likely to write letters in the homeland scenario, whereas increased technical skill and less support for nationalism were significant in the foreign country (Bagaria)

Table 4. Linear Regression Models for Total Number of Actions (N = 353)

	Physical actions						Cyber actions					
	Homeland			Bagaria			Homeland			Bagaria		
Variables	*B*	*SE*	β	*B*	*SE*	β	*B*	*SE*	β	*B*	*SE*	β
Patriotism	0.017	.017	.046	−0.002	.018	−.006	−0.023	.015	−.074	−0.002	.015	−.008
Nationalism	0.005	.037	.008	0.000	.038	.001	−0.052	.031	−.090	−0.018	.032	−.032
Group equality	−3.026	.019	.000	0.016	.020	.046	4.333	.016	.000	−0.017	.017	−.055
Out-group antagonism	−0.096	.026	−.209***	−0.037	.027	−.088	0.059	.022	.154**	0.013	.023	.035
Cyber actions	0.685	.052	.572***	0.581	.055	.504***						
Physical actions							0.488	.037	.585***	0.428	.040	.493***
Technological skill	0.047	.021	.099*	0.043	.021	.098*	−0.012	.018	−.030	−0.005	.018	−.014
Piracy	0.016	.029	.024	0.009	.030	.014	0.072	.025	.128**	0.070	.025	.130**
Country of origin	−0.732	.218	−.149***	−0.299	.211	−.066	0.414	.186	.101*	0.097	.190	.025
Gender	0.106	.145	.035	0.035	.148	.012	−0.213	.122	−.083	−0.287	.126	−.116*
Age	0.014	.019	.031	−0.010	.020	−.024	−0.016	.016	−.042	−0.013	.017	−.035
Constant	1.310	.784			1.013	.795		.789	.663		1.255	.681
R^2	.416			.295			.403			.290		

*$p \leq .05$. **$p \leq .01$. ***$p \leq .001$.

Table 5. Logistic Regression Models for Physical Actions (N = 353)

	Write a letter		Participate in a protest		Travel to protest		Confront an official	
Variables	Homeland	Bagaria	Homeland	Bagaria	Homeland	Bagaria	Homeland	Bagaria
Patriotism	.094**	.061*	−.023	.032	−.039	−.103**	.029	−.031
	(.037)	(.032)	(.037)	(.033)	(.036)	(.037)	(.039)	(.043)
Nationalism	−.056	−.136*	.056	.006	.074	.130	.023	.031
	(.078)	(.068)	(.076)	(.069)	(.075)	(.081)	(.079)	(.091)
Group equality	.029	.040	.025	.054	−.020	.001	.002	−.015
	(.040)	(.035)	(.041)	(.036)	(.041)	(.042)	(.041)	(.047)
Out-group antagonism	−.169***	−.033	−.151**	−.116*	−.188***	−.082	−.002	.066
	(.053)	(.048)	(.055)	(.049)	(.057)	(.060)	(.059)	(.064)
Cyber actions	.486***	452***	1.470***	.672***	1.266***	.623***	1.040***	.872***
	(.144)	(.116)	(.247)	(.143)	(.221)	(.116)	(.161)	(.134)
Technological skill	.085	.105**	.007	.002	.083	.073	.077	.080
	(.047)	(.040)	(.045)	(.040)	(.045)	(.044)	(.045)	(.050)
Piracy	.041	.003	.076	.060	.082	.003	−.030	.030
	(.065)	(.054)	(.066)	(.057)	(.064)	(.061)	(.064)	(.068)
Country of origin	−1.344***	−.188	−.638	−.693	−1.458**	−.781	−.949	−.277
	(.422)	(.398)	(.437)	(.410)	(.513)	(.609)	(.561)	(.595)
Gender	.136	.333	−.135	−.107	−.045	−.208	.450	.586
	(.301)	(.268)	(.304)	(.278)	(.302)	(.315)	(.324)	(.383)
Age	−.006	−.048	.016	.000	.021	.011	.050	.013
	(.040)	(.035)	(.039)	(.037)	(.039)	(.315)	(.041)	(.049)
Constant	−.405	−.665	−.386	−1.133	.378	−.455	−4.443**	−3.510
	(1.616)	(1.423)	(1.647)	(1.495)	(1.639)	(1.710)	(1.747)	(1.942)
Model χ^2	67.943***	42.538***	102.188***	59.079***	114.565***	59.323***	80.025***	67.137***
R^2	.248	.152	.343	.207	.371	.229	.288	.277

Notes: Unstandardized coefficients are presented with standard errors in parentheses due to space limitations. Pseudo R^2 are Nagelkerke R^2.
*p < .05. **p < .01. ***p < .001.

scenario. Protest participation was related to less support for out-group antagonism and willingness to engage in multiple cyber attacks spanning both models. These two items were also significant in the model for traveling to protest in the homeland model, along with those who considered the United States their home country. Those who reported lower levels of patriotism were more likely to travel to protest in the Bagarian scenario.

Within the cyber-attack scenarios, there were variations in the predictors based on the type of actions performed (see Table 6). As with the physical attacks, reporting a willingness to perform multiple activities in the real world was significant across all forms of cyber action. In fact, this was the

only predictor for posting messages on Facebook and other social media. Those who would engage in a web defacement of a government official's website were more likely to engage in piracy and multiple physical attacks, though individuals with more antagonistic views toward social out-groups were significant in the homeland model only. Participating in multiple physical attacks was significant across both models for defacing a government website, as was being male. Non-U.S. respondents were more likely to deface their own homeland's government website than respondents who considered the United States their homeland. Finally, individuals who were willing to search government servers for sensitive information were more likely to engage in both piracy and multiple forms of physical action. In the homeland model, individuals who did not hold patriotic ideals were more likely to engage in attacks as were foreign-born respondents. These items were not significant in the Bagarian attack scenario.

Discussion and Conclusion

The increasing global dependence on technology has dramatically increased opportunities for traditional and extreme forms of political action by civilians on- and offline. Few researchers have considered whether there are substantive differences in the predictors for willingness to engage in protests and other actions in their home country or foreign targets. This study sought to examine these issues using a scenario-based research instrument with an international sample of college students from a major Midwestern university. The findings suggest that few individuals were willing to engage in serious acts of violence in the real world and attacks against critical infrastructure in cyberspace against either their home country or a foreign nation. Two percent or less of the sample would utilize explosives to engage in an act of violence in the real world. Less than 2% would attack critical infrastructure online against domestic targets. This is in keeping with the extremely small number of individuals who engage in acts of terror or serious political violence (Martin, 2006).

In general, this study also suggests that nationalism and patriotism have a relatively limited affect on individual willingness to engage in cyber attacks and physical protests. In fact, strong support for patriotic ideals appears to only influence letter-writing behavior in the real world. Instead, individuals who do not support the suppression of minority and out-groups in society were more willing to engage in multiple attacks against their home nation, and forms of nonviolent action in the real world. Support for antagonistic relationships appears to influence multiple cyber actions within one's home

Table 6. Logistic Regression Models For Cyber Actions (N = 353)

	Post on Facebook		Deface officials' website		Deface government website search government servers			
Variables	Homeland	Bagaria	Homeland	Bagaria	Homeland	Bagaria	Homeland	Bagaria
Patriotism	.068	.028	−.026	−.002	−.098	−.074	−.156*	−.051
	(.041)	(.038)	(.054)	(.057)	(.060)	(.059)	(.060)	(.053)
Nationalism	−.105	−.031	−.118	−.100	.009	−.058	−.007	−.066
	(.085)	(.080)	(.117)	(.125)	(.128)	(.129)	(.131)	(.118)
Group equality	−.037	−.009	.036	.028	.034	−.006	−.057	−.029
	(.045)	(.043)	(.062)	(.063)	(.068)	(.065)	(.069)	(.060)
Out-group antagonism	−.093	−.077	.190*	.112	.109	.073	.066	.093
	(.059)	(.055)	(.094)	(.089)	(.102)	(.094)	(.102)	(.084)
Physical actions	.764***	.900***	1.285***	1.113***	1.459***	1.073***	1.219***	.576***
	(.117)	(.148)	(.215)	(.170)	(.254)	(.171)	(.226)	(.137)
Technological skill	−.004	.022	−.034	−.007	.003	−.028	−.125	−.019
	(.051)	(.048)	(.062)	(.064)	(.067)	(.066)**	(.072)	(.062)
Piracy	.056	.066	.204*	.150*	.281***	.216	.216**	.184**
	(.073)	(.070)	(.076)	(.078)	(.082)	(.080)	(.083)	(.074)
Country of origin	.344	−.270	1.026	1.120	1.820*	.722	1.850*	.231
	(.449)	(.435)	(.748)	(.685)	(.824)	(.764)	(.804)	(.683)
Gender	.011	.165	−.655	−.776	−1.116*	−.923*	−.358	−.688
	(.344)	(.321)	(.304)	(.441)	(.496)	(.463)	(.480)	(.441)
Age	−.022	−.031	−.096	−.072	−.135*	−.087	.074	.063
	(.044)	(.042)	(.062)	(.065)	(.071)	(.068)	(.064)	(.059)
Constant	1.024	1.005	−4.719	−4.002	−3.541	−1.494	−4.236**	−3.745
	(1.797)	(1.681)	(2.518)	(2.650)	(2.789)	(2.703)	(2.671)	(2.397)
Model χ^2	79.093***	70.455***	93.614***	82.591***	107.819***	82.645***	73.582***	40.395***
R^2	.305	.272	.428	.407	.503	.417	.395	.227

Note: Unstandardized coefficients are presented with standard errors in parentheses due to space limitations. Pseudo R^2 are Nagelkerke R^2.
*p < .05. **p < .01. ***p < .001.

country, and as well as for web defacements. Thus, the role of social attitudes may vary across virtual and real environments, in keeping with the larger literature on the contextual nature of violence and terror (Gurr, 1970; LaFree & Dugan, 2009; Martin, 2006; Taylor, 1993).

Participation in digital piracy was also a significant predictor for multiple forms of cyber action across both the homeland and Bagarian scenarios. Higher rates of piracy may serve as an indicator of overall willingness to engage in deviance in an online environment. Software and media piracy is a common form of cyber crime reported across college samples (Higgins, 2005; Hinduja, 2001; Holt et al., 2010; Skinner & Fream, 1997), and can be obtained with minimal technological skill, unlike certain forms of fraud and

hacking (Higgins, 2005; Skinner & Fream, 1997). Considering that technological skill was nonsignificant in all the cyber-attack models and negative, this study provides initial support for the notion that individuals need not have any real sophistication to motivate their pursuit of a politically motivated attack in a virtual environment. Individuals must simply desire to express themselves in an online environment and be willing to violate legal conventions in support of this goal.

There were also differences in individual action based on their country of origin. Those who identified the United States as their homeland were more likely to engage in multiple physical actions in the homeland model, whereas foreign respondents were more willing to engage in cyber attacks against their home country. This may be a function of the perception of risk in actions in the real world relative to cyberspace. There is generally greater tolerance for discussion and criticism of governmental policies and practices in the United States, enabling protest actions to take place in public settings without significant reprisal (Putnam, 2000). Political actions in cyberspace may, however, seem less risky for individuals from authoritarian regimes due to increased anonymity afforded by technology (Brenner, 2008). For instance, the recent Arab Spring across several countries in the Middle East demonstrates that political protests in the real world can be met with substantive violence to quell dissent (Stepanova, 2011). Further research is needed with a diverse sample of respondents from across the globe to clarify differences in the perception of physical attacks relative to virtual attacks where anonymity may help to mask the risk of detection from restrictive governments. Such data would better clarify the ways that the political system of an individual's country of origin may affect his or her willingness to engage in political action. Furthermore, the perceived likelihood of detection and successful outcomes from actions on- and offline was not explored in this study, making it difficult to assess how the risk of detection and punitive sanctions may affect individual willingness to engage in attacks. Further research is needed to clarify how the perceived risk of offending and punishment may affect willingness to engage in physical or cyber attacks.

The most significant predictors across both the linear and logistic regression models were the most extreme acts an individual was willing to engage in on- or offline. In fact, the number of attacks an individual reported was the only significant predictor for the most serious attacks against critical infrastructure. These findings clearly illustrate that among this sample of students, a willingness to engage in violence in support of political action cuts across the digital divide. An individual willing to commit an act of violence against a target in the physical world is also willing to attack a resource online. This

suggests that there may be a closer link between physical and cyber-based acts of terrorism than originally thought. Thus, law enforcement and intelligence agencies must investigate attacker activities using online sources and real-world information to better understand an individuals' propensity to engage in attacks in both virtual and real environments.

The relationships identified in this exploratory analysis provide a necessary step in increasing the knowledge of the relationship between on- and offline political action against both foreign and domestic targets. A great deal of additional research is needed, however, to expand the limited generalizability of these findings beyond this college sample. Developing samples from diverse groups within the general public, such as older individuals and those living in poverty, would help to clarify how economic conditions or exposure to technology influences willingness to engage in political violence in virtual and real spaces. Administering this survey to active hackers may also yield significant information on the role of technological sophistication and counterculture attitudes on individual willingness to engage in political action online.

In addition, the paucity of significant predictors in the models for attacks against Bagaria, whether on- or offline, demonstrates a need for additional research to clarify what behavioral and attitudinal factors may influence action against a foreign nation-state. This may be a consequence of model misspecification, or a need to better understand how various social factors affect the motivations to commit mass impact by physical or cyber-based attacks against nation-states. Such research can significantly clarify the relationship between extremist behaviors on- and offline, and any variations in the predictors for political violence generally.

Declaration of Conflicting Interests

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

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. Due to space limitations, it is not possible to discuss the myriad definitions for acts of terror (see Britz, 2010; Martin, 2006, for discussion) and cyber terror (see Britz, 2010; Denning, 2011). There is, however, substantive agreement that acts of terrorism can be viewed as political violence (see Schmid, 2004). Thus, we

will utilize the term *political violence* in lieu of terror where possible to conform to the general consensus on this issue.

2. Regression analyses could not be conducted for the most severe forms of attack against critical infrastructure including power grids and nuclear plants on- and offline due to the limited response rates for these items (see Tables 2 and 3).

References

Al-Rizzo, H. M. (2008). The undeclared cyberspace war between Hezbollah and Israel. *Contemporary Arab Affairs, 1*, 391-405.

Arquilla, J., & Ronfeldt, D. (1998). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: Rand.

Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 38-67). Hershey, PA: IGI Global.

Brenner, S. W. (2008). *Cyberthreats: The emerging fault lines of the nation state*. New York, NY: Oxford University Press.

Brewer, M. B. (1999). The psychology of prejudice: Ingroup love or outgroup hate? *Journal of Social Issues, 55*, 429-444.

Britz, M. T. (2010). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (Ed.), *Crime online: Correlates, causes, and context* (pp. 193-220). Raleigh: Carolina Academic Press.

Brodscky, J., & Radvanovsky, R. (2011). Control systems security. In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 187-204). Hershey, PA: IGI-Global.

Campos, J. A. D. B., Zucoloto, M. L., Bonafe, F. S. S., Jordani, P. C., & Maroco, J. (2011). Reliability and validity of self-reported burnout in college students: A cross randomized comparison of paper-and-pencil vs. online administration. *Computers in Human Behavior, 27*, 1875-1883.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the creation, distribution, and function of malware online*. Washington, DC: National Institute of Justice [Online]. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/230111.pdf

Conover, P. J., Searing, D. D., & Crewe, I. (2004). The elusive ideal of equal citizenship: Political theory and political psychology in the United States and Great Brittan. *Journal of Politics, 66*, 1036-1068.

Correll, S. P. (2010). An interview with anonymous. *PandaLabs Blog* [Online]. Retrieved from http://pandalabs.pandasecurity.com/an-interview-with-anonymous/

Curtin, R., Presser, S., & Singer, E. (2005). Changes in telephone survey non-response over the past quarter century. *Public Opinion Quarterly, 69*, 87-98.

Dalton, R. (2002). *Citizen politics: Public opinion and political parties in advanced institutional democracies* (3rd ed.). Chatham, NJ: Chatham House Publishers.

Denning, D. E. (2011). Cyber-conflict as an emergent social problem. In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). Hershey, PA: IGI-Global.

Dillman, D. A. (2007). *Mail and internet surveys: The tailored design method*. Hoboken, NJ: John Wiley.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social implications of the Internet. *Annual Review of Sociology, 27*, 307-336.

Duckitt, J. (2003). Prejudice and intergroup hostility. In D. O. Sears, L. Huddy, & R. Jervis (Eds.), *Oxford handbook of political psychology* (pp. 559-600). New York, NY: Oxford University Press.

Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior, 26*, 132-139.

Fishbein, M. J., & Ajzen, I. A. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Friedkin, N. E. (2004). Social cohesion. *Annual Review of Sociology, 30*, 409-425.

Gurr, T. R. (1970). *Why men rebel*. Princeton, NJ: Princeton University Press.

Herrmann, R. K., Tetlock, P. E., & Visser, P. S. (1999). Mass public decisions to go to war: A cognitive-interactionist framework. *American Political Science Review, 93*, 553-573.

Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*, 1-24.

Higgins, G. E., & Wilson, A. L. (2006). Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software. *Security Journal, 19*, 75-92.

Hinduja, S. (2001). Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice, 17*, 369-382.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*, 171-198.

Holt, T. J. (2009). The attack dynamics of political and religiously motivated hackers. In T. Saadawi & L. Jordan (Eds.), *Cyber infrastructure protection* (pp. 161-183). New York, NY: Strategic Studies Institute.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime & Justice, 33*, 31-62.

Huddy, L., & Khatib, N. (2007). American patriotism, national identity, and political involvement. *American Journal of Political Science, 51*, 63-77.

Jennings, K. M., & Zeitner, V. (2003). Internet use and civic engagement: A longitudinal analysis. *Public Opinion Quarterly, 67*, 311-334.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyber wars*. London, England: Routledge.

Kilger, M. (2011). Social dynamics and the future of technology-driven crime. In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology driven crime: Social dynamics and implications* (pp. 205-227). Hershey, PA: IGI-Global.

Kim, M. S., & Hunter, J. E. (1993). Relationships among attitudes, behavioral intentions, and behavior: A meta-analysis of past research Part 2. *Communications Research, 20*, 331-364.

Kosterman, R., & Feshbach, S. (1989). Toward a measure of patriotic and nationalistic attitudes. *Political Psychology, 10*, 257-274.

Kunovich, R. M., & Hodson, R. (1999). Conflict, religious identity, and ethnic intolerance in Croatia. *Social Forces, 78*, 643-668.

LaFree, G., & Dugan, L. (2009). Research on terrorism and countering terrorism. *Crime and Justice, 38*, 413-477.

Lavis, J., & Stoddard, G. (2003). Social cohesion in health. In L. Osberg (Ed.), *The economic implications of social cohesion* (pp. 121-149). Toronto, Ontario, Canada: University of Toronto Press.

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

Martin, G. (2006). *Understanding terrorism: Challenges, perspectives, and issues* (2nd ed.). Thousand Oaks, CA: SAGE.

Mummendey, A., Klink, A., & Brown, R. (2001). Nationalism and patriotism: National identification and out-group rejection. *British Journal of Social Psychology, 40*, 159-172.

Nagin, D., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review, 27*, 467-496.

Oakes, W. (1972). External validity and the use of real people as subjects. *American Psychologist, 34*, 329-339.

Payne, B. K., & Chappell, A. (2008). Using student samples in criminological research. *Journal of Criminal Justice Education, 19*, 175-192.

Pettigrew, T. F. (2003). Peoples under threat: Americans, Arabs, and Israelis. *Peace and Conflict: Journal of Peace Psychology, 9*, 69-90.

Piquero, A. R., & Bouffard, J. A. (2007). Something old, something new: A preliminary investigation of Hirschi's redefined self-control. *Justice Quarterly, 24*, 1-27.

Post, J. M. (1998). Terrorist psycho-logic: Terrorist behavior as a product of psychological forces. In W. Reich (Ed.), *Origins of terrorism: Psychologies, ideologies, theologies, states of mind* (pp. 9-25). Washington, DC: Woodrow Wilson Center.

Poulsen, K. (2011). In "Anonymous" raids, feds work from list of top 1,000 protesters. *Wired Threat Level* [Online]. Retrieved from http://www.wired.com/threatlevel/2011/07/op_payback/

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. New York, NY: Simon & Schuster.

Schatz, R. T., Staub, E., & Lavine, H. (1999). On the varieties of national attachment: Blind versus constructive patriotism. *Political Psychology, 20*, 151-174.

Schmid, A. P. (1988). *Political terrorism*. Amsterdam, Netherlands: North Holland Press.

Schmid, A. P. (2004). Frameworks for conceptualising terrorism. *Terrorism and Political Violence, 16*, 197-221.

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

Sears, D. O. (1986). College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of Personality and Social Psychology, 51*, 515-530.

Sibley, C. G., Robertson, A., & Wilson, M. S. (2006). Social dominance orientation and rightwing authoritarianism: Additive and interactive effects. *Political Psychology, 27*, 755-768.

Sidanius, J., & Pratto, F. (2001). *Social dominance: An intergroup theory of social hierarchy and oppression*. Cambridge, UK: Cambridge University Press.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime & Delinquency, 34*, 495-518.

Stepanova, E. (2011). *The role of information communications technology in the "ArabSpring": Implications beyond the region* (PONARS Eurasia Policy Memo No. 159) [Online]. Retrieved from http://www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf

Taylor, P. (1993). *States of terror: Democracy and political violence*. London, England: Penguin.

Terry, D. J., Hogg, M. A., & Duck, J. M. (1999). Group membership, social identity, and attitudes. In D. Abrams & M. A. Hogg (Eds.), *Social identity and cognition* (pp. 280-314). Oxford, UK: Blackwell.

U.S. Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Author. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf

Van Evera, S. (1994). Hypotheses on nationalism and war. *International Security, 18*, 5-39.

Van Laer, J. (2010). Activists online and offline: The Internet as an information channel for protest demonstrations. *Mobilization: An International Journal, 15*, 347-366.

Vasi, I. B. (2006). The new anti-war protests and miscible mobilizations. *Social Movement Studies, 5*, 137-153.

Verba, S., Schlozman, K. L., & Brady, H. (1995). *Voice and equality: Civic voluntarism in American politics*. Cambridge, MA: Harvard University Press.

Vollhardt, J. K., Migacheva, K., & Tropp, L. R. (2009). Social cohesion and tolerance for group differences. In J. De Rivera (Ed.), *Handbook on building cultures of peace* (pp. 139-152). New York, NY: Springer.

Wilson, C. (2008). *Botnets cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress* (Congressional Research Service Report RL32114). Washington DC: Congressional Research Service.

Wiltfang, G., & McAdam, D. (1991). Distinguishing cost and risk in sanctuary activism. *Social Forces, 69*, 987-1010.

Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology, 6*, 63-82.

Bios

Thomas J. Holt is an associate professor in the School of Criminal Justice at Michigan State University. His research focuses on cybercrime and the ways that technology and the Internet facilitate deviance. He received his doctorate in criminology and criminal justice from the University of Missouri-Saint Louis.

Max Kilger has been a member of the Spartan Devils Honeynet Project since 2008 and currently serves as the Chief Membership Officer for the Honeynet Project. He recieved his doctorate from Stanford University in Social Pscyhology in 1993.