Journal of Global Security Studies, 1(3), 2016, 235–247
doi: 10.1093/jogss/ogw006
Research Article

OXFORD

Repression, Education, and Politically Motivated Cyberattacks

Victor Asal,[1] Jacob Mauslein,[2] Amanda Murdie,[3] Joseph Young,[4] Ken Cousins,[5] and Chris Bronk[6]

[1]University at Albany, [2]Oklahoma State University, [3]University of Georgia, [4]American University, [5]University at Albany and [6]University of Houston

Abstract

What factors drive politically motivated cyberattacks? Our research focuses on one particular kind of cyberattack: politically motivated, distributed denial-of-service attacks (DDoS). We argue that denial-of-service attacks are a particular form of a larger category of political contention that is more similar to nonviolent than violent activism. We offer a country-level explanation that helps establish why some nation-states are more likely to suffer such attacks while most others are not. When we control for wealth and Internet penetration, the strongest factor explaining why a country is more likely to suffer DDoS attacks is the dangerous combination of repression and a highly educated population. The results have important implications both for the scholarly study of this form of contention, as well as for policy-makers grappling with this new form of activism.

Keywords: cyber, cyberattacks, repression

What factors drive politically motivated cyberattacks? There is a large and growing literature in computer science on cyberattacks (e.g., Hashmi, Saxena, and Saini 2012; Raghavan and Dawson 2011) and a growing literature on the increasing political threat of cyberattacks (e.g., Gandhi et al. 2011; Holt 2011; Buchan 2012; Valeriano and Maness 2014, 2015). Despite this increasing interest, there is very little quantitative research that looks at the political dimensions of cyberattacks, even with the strong policy argument that cyberattacks are becoming a growing security challenge for states (Nye 2011). One of the first empirical efforts looking at this challenge from an international perspective argues (with reason) that much of the "discussion of the concept of cyberwar, cyber conflict, and the changing dynamic of future security interactions is founded upon the study of what could be, conjured through spectacular flights of the imagination" (Valeriano and Maness 2014, 347).[1]

While Valeriano and Maness (2014, 2015) attempt to address this lacuna in the context of international rivalries and across an array of different kinds of cyberattacks, no existing work focuses on the specific characteristics that make a country an attractive target for a cyberattack, and extant scholarship has not developed a theoretical explanation of this phenomenon that connects it to a wider array of potential political nonviolent and violent actions. Additionally, existing empirical work does not examine the factors that make such attacks more or less likely. Addressing these shortcomings in the literature is necessary for informed policy recommendations on how best to protect online assets within a country from an attack.

Our research here focuses on one particular kind of cyberattack: *politically motivated*, *distributed denial-of-*

1 See also Valeriano and Maness (2012).

Asal, Victor et al. (2016) Repression, Education, and Politically Motivated Cyberattacks. *Journal of Global Security Studies*, doi:10.1093/jogss/ogw006
© The Author (2016). Published by Oxford University Press on behalf of the International Studies Association.
All rights reserved. For permissions, please e-mail: journals.permissions@oup.com

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

service attacks (DDoS). DDoS attacks are coordinated, broadly-based efforts intended to interrupt online communications. We examine why some countries are more likely to suffer such attacks while others (most others, actually) do not. This approach, focused on the target of the attack, is substantively important to generate a better understanding of this growing phenomenon. It also allows us to avoid the challenge of attributing attacks to other countries or non-state actors, which is extraordinarily difficult (Brecher 2012). Finally, it turns our focus away from cyberattacks as a potentially inflated threat for interstate warfare (Gartzke 2013; Lindsay 2014).

We argue that denial-of-service attacks are a particular form of a larger category of political contention.[2] DDoS attacks should thus follow the same strategic logic that drives other types of anti-government or anti-dissident actions within a state (Gurr 1970; Tilly 1978; Lichbach 1987; Olzak 1987; Moore 1995; Anderson and Mendes 2006). A country should be more likely to suffer a politically motivated DDoS attack when it violates the physical integrity rights of its own citizens and when it has a highly educated population. Repression by the government provides incentives for action. In an environment where the door is closed to other forms of nonviolent contention, the Internet has created a new resource for people to protest in ways that are nonviolent. Education affects people's ability to use this new resource. The ease with which attacks can be "anonymized" (e.g., distributed across thousands, even millions, of infected computers, à la botnets) means that both state and non-state actors alike can act with relative impunity. A repressed and educated population can politically protest from their laptops, a repressive government may be a likely target of attacks from abroad, and a repressive regime can act to limit speech, while maintaining plausible deniability.

Using novel data on DDoS attacks, we find support for this argument that domestic education levels and repression influence the likelihood of a DDoS attack on a country in a given year. Additionally, we find that *material* nonviolent contention is positively associated with politically motivated DDoS attacks, while violent contention is not associated with such attacks.

Our analysis focuses on DDoS attacks because they are both effective and one of the easier types of cyberattacks to carry out, and thus should reduce the mobilization costs for potential dissidents (Bronk 2008; Lesk 2007; Goth 2007; Nazario 2009; Clarke and Knake 2010; Mansfield-Devine 2011). As Sauter (2014, 10) points out:

> At its most basic level, a denial-of-service action seeks to render a server unusable to anyone looking to communicate with it for legitimate purposes. Complex or sophisticated tools are not necessary to launch a DDoS action. A group of people reloading the same website again and again at the same time could constitute a manual DDoS action, if they intend to bring that site down. However, automated tools and methods are much more effective against websites that rely on today's web infrastructure.

Distributed cyberattacks—cyberattacks across multiple sources—are an easy, low-risk means for educated, repressed people to express dissent or for a state to try to quell mobilization by this educated population. In what follows, we first outline denial-of-service attacks, what they are, what we know about them, and what we do not. We then discuss how cyberattacks fit into a larger repertoire of contentious actions in a particular society. From this discussion we derive particular hypotheses. We then discuss the DDoS data, how they are collected, how they are novel, and their limitations. Using these data, we then perform cross-national quantitative tests to test our hypotheses. We provide the estimates and substantive impacts of these factors that increase or decrease the likelihood of a DDoS attack. In the conclusion, we discuss limitations and future research in this area.

DDoS and the Growing Fear of Cyberattacks

It has long been clear that dependence on the Internet makes people vulnerable in new ways, a notion that social scientists are just now studying in a rigorous, systematic manner. As early as 1971, scholars theorized that computers could be used for malicious purposes (Vandevoort 1971). Since then, the Internet has become increasingly utilized as a conduit of exploitation and violence, and terms such as "cyber-war" and "cyber-terrorism" have entered our lexicon (Di Camillo and Miranda 2011). In this paper, we specifically focus on politically motivated DDoS attacks. We define these forms of cyber action as intentional efforts to limit the accessibility of online resources, where some form of political motivation is evidenced. We restrict our focus to DDoS attacks because if we are right that these are a new form of contentious politics, they should fit within our understanding of the factors that influence other types of contentious

2 Given the difficulty of attribution, we should note that it is possible that some of these attacks were carried out by state actors against other states or against non-state actors.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

politics, like on-the-ground nonviolent and violent protests within a country.

While the number and severity of DDoS attacks continues to increase year after year, there is very little peer-reviewed social science literature on denial-of-service attacks generally, and even less that examines cross-national statistical evidence. Compared to other subjects within contentious politics and international relations, the role of the Internet—and DDoS attacks in particular—is understudied and, as a result, under-theorized (Holt 2011). Part of the reason for this imbalance is the highly technical and rapidly changing character of the Internet generally, and DDoS attacks in particular. Academic research into DDoS attacks tends to approach the problem from a computer science lens, focusing on methods of detection and deterrence (Lee et al. 2008; Xiang et al. 2004; Jin and Yeung 2004) and tracing attacks to their true source (Law, Lui, and Yau 2005; Wheeler and Larsen 2003).

The general terrain of hackers and their motivations have also been explored (again, largely within technical disciplines), with some researchers framing the behavior as deviant and motivated by a need to rebel, to be defiant, and to boost self-esteem (Suler and Phillips 1998; Suler 1997). Other work on hacker motivations, however, rejects the pathological viewpoint and explores the sociology of hackers. Jordan and Taylor (1998) place the behavior in the context of community formation, with hacking as instrumental to the construction of in-groups and out-groups, that is, hackers and the computer security industry. But again, we have found almost no analysis that uses country-level data and takes into account country-level factors to explain the motivations of cyber attackers.[3] The scarcity of social science research highlighting the influence of domestic and international politics on denial-of-service attacks is unfortunate. This is particularly true given the assertion that DDoS attacks have acquired increasing significance in politics and for national security policymakers (Hoover 2012).

Numerous episodes throughout the past 20 years stand as exemplars as to how cyber politics have become significant security concerns for both non-state and state actors. Two early examples of politically motivated DDoS attacks occurred in the late 1990s, the first of which was orchestrated by Spanish protestors. In 1997, cyber activists flooded the Institute for Global Communications (IGC) with thousands of emails because the company hosted the Euskal Herria Journal website, a publication that supported Basque independence (and, by extension, the ETA terrorist group). The IGC was eventually forced to relent to protestors' demands, as their ability to service its other customers had been severely impacted (Denning 2011).

Similar tactics were employed in 1998 by the Tamil Tigers, a Sri Lankan terrorist organization. Targeting Sri Lankan embassies around the world, the group sent 800 emails a day for two weeks in an effort to crash government servers. Each of the emails read "We are the Internet Black Tigers and we're doing this to disrupt your communications" (Denning 2001, 74). Intelligence authorities often cite this DDoS attack as the first digital assault against a country's computer system by a terrorist organization (Denning 2011).

DDoS became widely known to the American public in February 2000 when a series of attacks was launched against the Yahoo!, Amazon.com, Dell, eBay, and CNN websites. In that case, the perpetrator was a Canadian teenager, but throughout the decade DDoS became an increasingly viable tool for international coercion (Hersher 2015).

Perhaps the most famous uses of DDoS attacks occurred in Estonia and Georgia, spurred on by deteriorating political conditions with Russia. In 2007, Estonia was the target of politically motivated DDoS attacks from Russian hackers after the country announced its intention to move the Bronze Soldier of Tallinn statue. The hackers responded to the announcement by using an estimated 1 million computers located in over 75 countries to mount the massive assault (Jones and Kovacich 2016). In 2008, during a brief armed conflict between Georgia and Russia, numerous Georgian websites were targeted and knocked offline. In both cases, the Russian government denied involvement. Instead, the nationalistic Nashi Youth movement claimed responsibility for the Estonian attacks, and it was among a number of groups suspected of orchestrating the Georgian attacks as well.

More recently, in February 2012, hackers affiliated with the hacktivist community "Anonymous" claimed responsibility for initiating a DDoS attack against the website of the US Central Intelligence Agency. The attack was launched as a response to perceived inactivity by the US government in stopping online child pornography. In a statement released by Anonymous, the group explained that the attack "created a way more significant amount of attention to a situation that goes unnoticed far too often" (Biddle 2012, n.p.).

A few years later, in October 2015, several websites associated with Thailand's government were disabled by a DDoS attack after Thai officials announced that a single Internet gateway would be imposed in an effort to block "inappropriate websites" and to control the flow of infor-

3 An important exception is Valeriano and Maness (2012, 2015).

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

mation from abroad. According to the BBC News (2015, n.p.), "Thai netizens insist this is not an attack, but a form of civil disobedience," which further reiterates how the Internet can be used as a twenty-first century tool of contentious politics.

These cases illustrate how cyber events are coming to occupy a position of prominence in political conflict and activism. But questions abound regarding how cyber issues should be addressed in international relations and how academic theories may apply to cyber politics. We are still in an early phase of understanding how the power relationships in cyber politics (perhaps most significantly, deterrence) function (Nye 2011; Libicki 2009). But to simply cast cyber incidents as threats requiring state action limits our analysis. As the examples above demonstrate, the Internet is a tool for more effective and public displays of political conflict for non-state actors as well. As a result, it is vitally important for us to focus attention on how the Internet is changing the possibilities for political conflict and the dynamics between state and non-state actors in this space (Adamson 2016).

Does Cyberspace Change Politics?

While some see cyberspace as simply a reflection of the physical world (Norris 2001), we believe that in fundamental ways the creation of a virtual terrain has changed the physical environment, and in particular the landscape for contention (Kellner 2003; Chadwick 2006). When thinking about the impact of this virtual environment on contention, we draw upon Lichbach's (1998) notions of dissident action and rational rebel behavior, especially his insight that dissident groups must produce innovations in technology in order to effectively challenge opponents that otherwise have greater resources. We believe that DDoS attacks can be considered innovations in dissident group technology. Lichbach's "rebel's dilemma" focuses on the limitations to mobilization based on the potential cost of action versus the benefits that one can receive if those efforts are successful. Denial-of-service attacks in particular offer two significant changes to the rebel's dilemma: (1) they are very low-cost means of disrupting opponents' communications, and (2) they dramatically reduce the likelihood of discovery (McCarthy and Zald 1977). Many politically motivated cyber attackers have tried "to show the general public and the media that they are standing up against the establishment to protect the rights of people around the world that are endangered by national or corporate oppression and greed" (Still 2005, 1). In other words, many cyber attackers are behaving like other political activists and political dissidents; they are using their continuous actions in support of a political message.

How, then, do cyberattacks fit into the repertoire of political contention? The opportunity structure literature suggests that choices of contention will be impacted by the nature and behavior of the regime in question, which will create opportunities or constraints on action (Tarrow 1998; Tarrow and Tilly 2007). The human rights literature also suggests that regime type constrains the state's use of repression and the lack of repression opens up room for dissenters to use nonviolent means (Poe and Tate 1994; Davenport and Armstrong 2004). More important than regime type, though, we believe that repression itself should be a key factor in encouraging DDoS attacks in a country. Even strong democracies sometimes repress dissidents (Gurr and Moore 1997, 1083; Davenport 2007).

Why should repression, then, be associated with DDoS attacks? First, repression closes the door to many forms of nonviolent contention and "regular" politics. It thus leaves dissenters looking for alternate routes of behavior (Tilly 1978; Gurr 2000; Regan and Norton 2005; Saxton and Benson 2006). Second, cyberattacks are a relatively safe way to engage in resistance when the government is repressing. They are an attractive tool, similar to what Collier et al. (2003, 74) suggest about the willingness of diasporas to mobilize, as they "do not suffer the consequences of violence" because attributing such attacks is hard to do. Repression, though, is not just a constraint on mobilization. It can spur mobilization in the direction of contentious—and anonymous—behavior. Repression also creates grievance and, as such, should drive more individuals and organizations toward contention of all sorts (Davenport 2007).

State repression has been linked to increases in many other types of political violence. For example, Walsh and Piazza (2010) found that repressive regimes are more likely to be targeted with transnational terrorism, as governments that frequently use repression are less likely to get the necessary intelligence to thwart terrorist attacks. State repression has also been linked to interstate conflict; the behavior a state uses toward its own population affects its interactions internationally (Sobek, Abouharb, and Ingram 2006). As such, not only could repression drive DDoS attacks by non-state actors within a state, it could also affect the likelihood of attacks against a state from international non-state and state actors.

Repression, though, is only one component of the picture. There is a strong body of literature that suggests that resources are a key determinant of what dissenters will or will not do (Collier and Sambanis 2002; McCarthy and Zald 1977). Clearly the level of Internet penetration is pivotal, but we believe that another critical factor is the level of education in a population. When repression

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

pushes people away from protests or sit-ins, educational attainment gives people the wherewithal to use cyber tools to engage in nonviolent action if they have the connections to do so. Much of the literature that examines protests points out that higher education makes individuals more likely to protest, and countries with a highly educated population are more likely to experience nonviolent contention. For example, when examining the impact of democratic elections on citizens' propensity to protest, Anderson and Mendes (2006, 103) found that "[e]ducation also had a significant and positive effect on people's propensity to engage in protest—those with higher levels of education were much more likely to do so." In a study of seventeen Latin American countries, Machado, Scartascini, and Tommasi (2011) found that higher education levels encouraged protest.[4] Corrigall-Brown (2011) explicitly identified education as a key resource for protest by arguing:

> Resources are important predictors of both whether or not one ever engages and one's trajectory of participation over time. Those with higher levels of education and knowledge are more likely to have ever engaged and to persist. These cultural resources both prime individuals to participate and keep them active over time. (57)

Olzak (1987) also pointed to education as an important resource for mobilization. Klesner (2009) saw a lack of education as a key resource constraint. While all of these examples are focused primarily on nonviolent contention, there is a literature that argues that the same positive relationship between education and contention should be related to violent contention as well in the arena of terrorism (Abadie 2004; Akyuz and Armstrong 2011; Berrebi 2003; Krueger and Malečková 2003; Krueger and Laitin, 2008) and ethnic conflict (Lange 2011; Lange & Dawson 2010).

We believe that the resource implications of education should be stronger for cyber-contention because there is a direct link between the ability to engage in such activity and one's educational attainment. Carrying out these attacks does require some individual and collective intelligence. In this regard, our argument connecting education to DDoS attacks is somewhat different from the arguments regarding education in the literature provided above. In the literature on nonviolent protest and terrorism, education's role is one of political engagement and the likelihood of joining associations and political groups. In the case of DDoS attacks, these arguments may still apply but education also directly affects the likelihood that individuals will have the skills to carry out these attacks.

There is evidence that cybercrime in general is tied to higher levels of education (Neufeld 2010). In a study of forty "Yahoo boys," a Nigerian cybercrime gang, Aransiola and Asindemade (2011) found that all forty members had either an undergraduate or a postgraduate degree. The authors speculated that, since Nigerian youths below the postsecondary education level rarely have access to computer technology, higher institutions of learning—where computers are readily available—are "breeding grounds" for cybercriminals. This finding is backed up by the Indian National Crime Records Bureau, which noted that 66 percent of those individuals accused of committing computer crime in 2012 were "youths who are educated and tech-savvy" (Narayan 2013). Additionally, from 1999 to 2004, of the total number of cybercrimes reported to Taiwanese police, nearly one-fourth of the suspects had a college diploma (Lu et al. 2006).

Ultimately, readily available access to computers and the Internet, as well as the education required to operate such technology, are vital components of cybercrime activity. When exploring the global digital divide, education is a key factor in computer penetration rates (Chinn and Fairlie 2007). As pointed out by Aransiola and Asindemade (2011), many Nigerian youths who do not receive postsecondary education are not equipped with the computer knowledge necessary to commit any form of sophisticated cybercrime. Thus, we can extrapolate that in some developing states, education is a key factor in general computer access, as well as the ability to commit Internet attacks for political motives. Likewise, countries with a highly educated population are likely to be better targets for international DDoS attacks; these would be the countries where Internet use is widespread and such an attack could interfere with the day-to-day interactions of an educated workforce and political dealings.

Thus, we hypothesize that, even when controlling for key factors like GDP per capita and Internet penetration:

H1: As education levels increase, Internet resources within a country are more likely to suffer a DDoS attack.

H2: As repression increases, Internet resources within a country are more likely to suffer a DDoS attack.

In the next section, we discuss data on DDoS attacks and how we test the above hypotheses. These data provide a cross-national examination of this form of contention, but there are limitations, which we address.

4 See also Schofer and Longhofer 2011; Beissinger, Jamal, and Mazur 2012; Sherkat and Blocker 1994; Pichardo Almanzar and Herring 2004; Martinez 2008; and Waldner 2001.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

Table 1. Example of DDoS attack from source material

Source	Date published	Notes
ArabianBusiness.com	8/12/2008	Authorities in Georgia claim that the Russians launched a coordinated campaign of distributed denial-of-service (DDoS) attacks against many Georgian government websites on Friday, when armed hostilities broke out.

Collecting Data on Political DDoS Attacks

In order to measure our dependent variable, our initial goal was to establish the most comprehensive record of politically motivated DDoS attacks. We searched all English-language news sources indexed by LexisNexis[5] during the period of study to ensure the broadest available coverage that was readable and understandable for our coders. We focused on the period of time from January 1, 1998, to February 3, 2011 (the final date of data gathering), for reasons of tractability, as well as the knowledge that there were relatively few DDoS attacks in the early years of the Internet. Because our focus is on distributed denial-of-service attacks, we searched on that exact phrase and its abbreviated form, "DDoS."

These queries produced a total of 5,041 articles[6] (31.4Mb) from 771 sources, including major newspapers, newswire services, broadcast transcripts, government news and transcript services, computing and business industry journals, and computing industry blogs. After reformatting for consistency, we imported these into Provalis ProSuite, a leading text analytics software package.[7]

As would be expected, many of the texts mention DDoS attacks only briefly (e.g., broad discussions of cyber security issues). To focus our efforts only on the most relevant text segments, we used WordStat, a program within the ProSuite software, to identify and extract all paragraphs containing the original target terms. This resulted in 6,296 paragraphs, each of which we associated with the metadata of the source article. We then exported these as a spreadsheet for review by human coders (see the example in Table 1).

Coding DDoS Attacks

We define DDoS attacks as coordinated, broadly based efforts (successful or otherwise) to interrupt online communications. This does not include instances where governments or industry block specific websites or platforms (i.e., "blackouts"), where such outages are accidental or the result of "flash events" (e.g., "slashdotting"), or where an individual is able to tie up a web server through technical exploits (e.g., "ping flooding").

Given that defining *what is political* can be a highly subjective exercise, we also deemed it necessary to develop a consistent rubric for determining whether we should consider an attack *political*, as well as assessing the degree to which it fits into this category. We began with an understanding that attacks involving state institutions and state actors as either targets or perpetrators are quintessentially political. We also considered attacks that broadly target many or most networks throughout a nation-state to be political; these would be analogous to conventional attacks on infrastructure.

In addition, we considered attacks on the websites of active and aspiring political actors (e.g., electoral candidates), as well as those in which governance concerns are discussed, to be political in nature, though of a different order than those directly involving states or state institutions. We assessed attacks where non-state attackers were said to have been acting in defense of political rights (as understood by the perpetrators), or in opposition to alternative ideologies or identities (political, cultural, ethnic), in a similar manner.

The targets of DDoS attacks are generally identified in the source texts, though often in rather general terms (e.g., "government and banking websites"). This is less true of attackers' identities—attribution being a persistent problem on the Internet, as already noted. However, whenever information on the attacker was available, we noted it.

Similarly, the national territory in which a target resides was usually noted, although it was not always clear

5 We chose LexisNexis Academic Universe® for the breadth of its coverage, as well as the ability to access full-text articles throughout the period of interest.

6 After removing likely duplicates, identified as articles with identical word counts, published on the same day by the same source. The original queries returned 5,315 articles—more recent queries show a dramatic increase in the number of articles per year, jumping from an average of 3.7 per day in 2010 to 11.5 per day in 2011 and 12.9 in 2012. DDoS attacks are gaining salience, if nothing else.

7 Details about Provalis software, including a list of academic, governmental, and commercial users, are available at http://provalisresearch.com.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

Table 2. Most-targeted countries, based on raw numbers of DDoS attacks in sample

Country	Number of attacks	Percentage of total
United States of America	63	20.1%
Russia	35	11.1%
Myanmar	21	6.7%
Tunisia	18	5.7%
United Kingdom	15	4.8%
China	14	4.5%
Republic of Korea	14	4.5%
Vietnam	13	4.1%
Mexico	10	3.2%
Belarus	9	2.9%

whether the targets' websites were also hosted in those same countries. Wherever this was identified, we noted the alternative "target location" in brackets. These were later separated out as an alternative mapping of attack targets; attacks where no extra-national hosts were identified were assigned to the country in which the target is resident.

Due partly to the often long periods between an attack and reliable attribution, public reporting on any specific cyberattack is often spread over weeks, months, or even years. In developing a broad record of DDoS attacks, this meant we often had multiple reports on the same event, each with only partial information about our key variables. In practice, therefore, after coding for all the information available in the text extracts, we needed to consolidate these multiple reports into a unified record that included the full range of what was publicly known about the attacks. Sorting by the date the attacks began, and then filtering by the national territory of the target and/or target name, we created composite records that combined the most detailed information for a given attack, as well as the supporting sources and text extracts. This resulted in 314 recorded attacks between 1998 and 2010, involving fifty-one different target countries, and forty-six countries from which attacks were believed to have originated.[8] See Table 2 for a list of the most-targeted countries in our sample. Entities within the United States—both governmental and non-governmental—were the most common targets in each data set.

8 Even at the state level, attribution was very difficult to determine—attackers or host countries were unidentified in fully 42 percent of all reported attacks.

Transformation for Analysis

Following this procedure, we had a rich source of data about the use of DDoS attacks for political purposes. To prepare the data for cross-national, time-series analyses, we then aggregated attacks annually, based on target-country and host-country values. This resulted in 123 individual country-year records for the target-country data set (with 1 to 16 attacks recorded per year), and 134 such records for the host-country data set (with 1 to 23 attacks). For this project, the target-country count of DDoS attacks is used as our dependent variable. While we hope that future research will also use the data on host-country values, our hypotheses concern only the targeted country and thus are best examined with a focus on the target-country data.

Additional Variables for Future Research

In addition to the total number of attacks within a given nation-state each year, we developed dichotomous codings for the target "types": government entities; non-state political actors (e.g., candidates) or political discourse; journalism and media; ethno-religious identities or discourse; economic actors; actors active in intellectual property issues; and infrastructure (including Domain Name System (DNS) and Internet service providers). We also noted the proportion of attacked websites, which were hosted externally.[9] We hope that these indicators will be useful to future projects.

Key Independent Variables

To test our hypotheses, we also needed variables that captured the concepts of (a) education levels for potential attackers, and (b) state-perpetrated human rights violations within the country attacked, as well as controls for more traditional forms of anti-government protest. To test the first concept, we utilized a measure of the average number of years of education for males in the state. This variable, which comes from the Institute for Health Metrics and Evaluation, captures the years of formal schooling in men aged 25 and older (Gakidou et al. 2010). Since there are no known females convicted as perpetrators of a

9 Though not relevant for the analysis here, we also identified the proportion of attacks said to have originated internally to a country (e.g., cyber own goals), and also the national territories from which attacks were said to have originated, and we developed dichotomous codings for attacker type: government; organized crime; non-governmental organizations; Anonymous (à la 4chan); and hackers (when such information was available).

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

DDoS attack, the use of male education rates closely matches the likely population of potential attackers. We use years of formal schooling for men 25 and older to account for variation in formal education start dates cross-nationally and because of its wide usage in the literature (Collier and Hoeffler 2004).

Our second concept of interest, human rights violations by state actors, is captured by the inclusion of the CIRI Human Rights Dataset index of physical integrity rights (Cingranelli, Richards, and Clay 2014). This nine-point index (0 to 8) captures government violations of freedom from torture, political killing, political imprisonment, and political disappearance. For our purposes, the index has been reversed from its typical ordering to aid in interpretability; in our models, a higher score on this index equates to more widespread physical integrity rights violations. This scale is coded yearly based on reports from the US State Department and Amnesty International (Cingranelli, Richards, and Clay 2014). We use the CIRI physical integrity rights scale for two reasons. First, we use it because it conforms to our concept of interest: the repressive practices of state governments against their citizens. Additionally, the CIRI physical integrity scale has been used as the key independent variable in studies that focus on many other forms of contentious politics, including terrorism (Walsh and Piazza 2010), protest (Bell et al. 2013), and interstate war (Sobek, Abouharb, and Ingram 2006).

A number of control variables were also included in the statistical models. For anti-state violence, we followed Murdie and Bhasin (2011) and used separate counts of the number of violent and nonviolent protests by domestic individuals or groups against their government or government agents. These data, also used in Bhasin (2008), are based on event data coded from Reuters Global News Service reports as part of the Integrated Data for Event Analysis (IDEA) project (Bond et al. 2003). We utilized an updated version of these variables from Bell et al. (2013). To account for any over-reporting of protests simply due to an overabundance of media reports about a country, we included the natural log of the total number of reports in Reuters about the country in that particular year as an additional control.

Additionally, we included the Polity IV revised combined polity score, often referred to as Polity 2 (Marshall, Jaggers, and Gurr 2011). This measure captures a country's position on a 21-point regime-type continuum, varying from –10 for a full autocratic regime to +10 for a consolidated democracy. Controls for natural log of population size and GDP per capita were also included and came from the Penn World Table (Heston, Summers, and Aten 2012). In addition, we added a control for the number of Internet users per 100 people from the World Development Indicators (World Bank 2012). For several of these variables, we used the Quality of Governance aggregated data set (Teorell et al. 2011).

Research Design and Analysis

To evaluate how the above risk factors influence a country experiencing a denial-of-service attack, we estimated a logistic regression. As King and Zeng (2001) note, to avoid bias when we study rare events, we should correct for the fact that a positive value of the dependent variable is infrequent as compared to zero. They suggest estimating a rare-events logit (King and Zeng 2001, 138), as a traditional logistic regression can "sharply underestimate the probability of the rare event, and commonly used data collection strategies are grossly inefficient." In short, the rare events logit can produce more accurate estimates of the probability of the rare event (a DDoS attack). As discussed above, we constructed a comprehensive framework for collecting the dependent variable, the denial-of-service attack. While we have complete cases for this variable, we lose information due to missingness in the independent variables and controls. Given this problem, one approach is to delete these cases (listwise deletion). If any of these data are missing due to observable factors, then the case selection criteria will lead to biased estimates (King et al. 2001). We estimated models using both multiple imputations to recover the missing data and listwise deletion. To impute the data, we used Royston's (2005) method of chained imputation.[10]

Table 3 provides the coefficient estimates and standard errors for each variable across three models. Model 1 uses multiple imputations to recover lost data and thus produces estimates adjusted over five separate data sets. Model 2 also uses data across five multiple imputed data sets, but also includes year-fixed effects to control for specific temporal factors. Model 3 utilizes one data set that deletes cases where any variable has a missing value. The estimates for each independent variable are consistent across the three models. The coefficients vary slightly in size, but the direction and significance of the relationship holds. A few of the controls change in size and significance across the three models, suggesting that there may be bias in their estimate in Model 3.

10 This method of multiple imputation is native to Stata 12. Horton and Kleinman (2007) provide a comparison of the different multiple imputation methods and software.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

Table 3. Determinants of political denial of service attacks in the world, 1998–2010

VARIABLES	(1) Imputed data	(2) Imputed with year fixed effects	(3) Missing data
Years of ed. (Male)	0.180**	0.243***	0.264***
	(0.0744)	(0.0817)	(0.0873)
Human rights violations	0.214***	0.189**	0.203**
	(0.0766)	(0.0897)	(0.0968)
Democracy	–0.0359	–0.0463*	–0.0672**
	(0.0228)	(0.0257)	(0.0332)
Population	0.442***	0.202	0.337*
	(0.142)	(0.178)	(0.198)
GDP	0.702***	0.236	0.277
	(0.240)	(0.244)	(0.340)
Internet users	0.00818	0.0134	0.0246**
	(0.00804)	(0.0105)	(0.0116)
Nonviolent protests	0.0325**	0.0309**	0.0247**
	(0.0135)	(0.0121)	(0.00999)
Violent protest	0.000941	0.000120	–0.00292
	(0.00417)	(0.00330)	(0.00282)
Total news reports	–0.276**	0.0968	–0.138
	(0.132)	(0.171)	(0.159)
Constant	–14.06***	–12.10***	–11.33***
	(2.524)	(2.327)	(3.253)
Observations	2,028	2,028	1,566

Robust standard errors in parentheses clustered on country.
***$p < 0.01$
**$p < 0.05$
*$p < 0.1$

Results

Controlling for wealth and Internet penetration, we find that countries are more likely to suffer DDoS attacks (1) if the male population is more educated; (2) as repression increases; and (3) in countries with more nonviolent contention. These results hold regardless of the model (Models 1–3). These results provide strong support for our hypotheses.

A country's wealth, captured by GDP per capita, is generally positively associated with the probability of a DDoS attack, although the result is not significant in the model with fixed effects (Model 2). The level of democracy is negatively associated with DDoS attacks, but in the imputed data with fixed effects (Model 1) this result cannot be distinguished from zero. The results for population are similarly mixed. In two of the three models, larger populations are associated with more attacks, but not when using fixed effects controlling for country-specific factors. The number of Internet users in the imputed data is not associated with attacks, but it is in the data using listwise deletion (Model 3). We are skeptical due to the sensitivity of this result.

Interestingly, the probability of a DDoS attack is not correlated with violent contention. Across the three models, the sign flips; the coefficient is small and never significant. Figure 1 shows the results of simulations to predict the probability of a DDoS attack given a change in the independent variables from their minimum to maximum.[11] As the figure shows, the predicted effect of nonviolent protests has the largest impact on predicting an attack (from 64 to 100 percent more likely). Moving from low to high wealth leads to an expected change in the probability of an attack by 32 percent, on average. On average, a change from low to high education also increases the probability of an attack by 9 percent. Increasing human rights violations from their minimum to their maximum also increases the probability of an attack, on average, by 6 percent.

Conclusion

What determines politically motivated DDoS attacks? Although there has been significant policy attention to the topic, with few exceptions political science has remained silent on the determinants and outcomes of so-called cyberattacks. In this paper, we argue that politically motivated DDoS attacks are one of a series of contentious behaviors that states and dissidents have in their repertoires. DDoS attacks are just another useful tool in the repression–dissent nexus. Like other forms of nonviolent protest, would-be dissidents choose DDoS attacks when it matches their particular skill sets and motivations. As such, when repression within a state is high and when education levels enable the use of technology that facilitates DDoS, a country is more at risk for an attack. As discussed, this logic also implies that a repressive state will be more likely to use DDoS attacks on its educated population. We test the implications of this logic using newly coded data on DDoS attacks from 1998 to 2010 and find much support for our central hypotheses.

What do these results imply for policy? First, we take these results to indicate that focusing on the *new* threat of cyberattacks could be overstated. Instead of being a *new* threat, DDoS attacks are simply a new tool for dissident-state relations that reflect long-standing determinants of other nonviolent political actions. Second, we see this research as important in the formation of any counter-cyber efforts. Like research on terrorism, actions taken by states

11 This figure uses estimates from all five imputed data sets and utilizes CLARIFY to combine the estimates (Boehmke 2008).

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

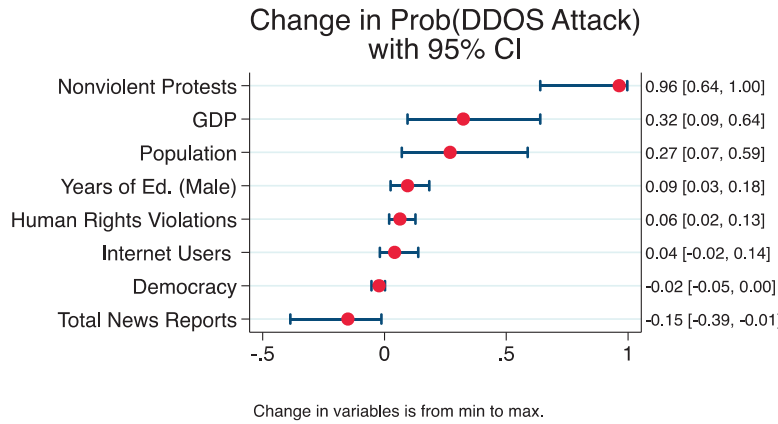

Figure 1. Change in predicted probability of a denial of service attack

that restrict the rights and abilities of an educated population may increase the pool of potential attackers (Bueno de Mesquita 2005). Counter-cyber efforts that restrict the abilities of an educated population to utilize their skills may end up mobilizing the population against the state.

Finally, we see these results as important because they stress the need for cross-disciplinary work. Understanding the risks posed by cyberattacks to states requires more than just understanding technological vulnerabilities. It requires a focus on the motivations for all types of contentious political actions, including hacking. We hope researchers can draw on this work and the data set underlying our results in future work.

Replication Data

Replication data can be found at http://www.isanet.org/Publications/JoGSS/Replication-Data.

References

Abadie, Alberto. 2004. *Poverty, Political Freedom, and the Roots of Terrorism*. Cambridge, MA: National Bureau of Economic Research.

Adamson, Fiona B. 2016. "Spaces of Global Security: Beyond Methodological Nationalism." *Journal of Global Security Studies* 1(1): 19–35.

Akyuz, Kadir, and Todd Armstrong. 2011. "Understanding the Sociostructural Correlates of Terrorism in Turkey." *International Criminal Justice Review* 21(2): 134–55.

Anderson, Christopher J., and Silvia M. Mendes. 2006. "Learning to Lose: Election Outcomes, Democratic Experience and Political Protest Potential." *British Journal of Political Science* 36(1): 91–111.

Aransiola, Joshua Oyeniyi, and Suraj Olalekan Asindemade. 2011. "Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria." *Cyberpsychology, Behavior, and Social Networking* 14(12): 759–63.

BBC News. 2015. "Thai Government Websites Hit by Denial-of-Service Attack." *BBC News Asia*, accessed October 1, 2015, http://www.bbc.com/news/world-asia-34409343.

Beissinger, Mark R., Amaney Jamal, and Kevin Mazur. 2012. "Who Participated in the Arab Spring? A Comparison of Egyptian and Tunisian Revolutions (2012)." APSA 2012 Annual Meeting Paper. http://ssrn.com/abstract=2108773.

Bell, Sam R., David Cingranelli, Amanda Murdie, and Alper Caglayan. 2013. "Coercion, Capacity, and Coordination: Predictors of Political Violence." *Conflict Management and Peace Science* 30(3): 240–62.

Berrebi, Claude. 2003. "Evidence About the Link Between Education, Poverty and Terrorism Among Palestinians." Princeton University Industrial Relations Section Working Paper 477. http://ssrn.com/abstract=487467.

Bhasin, Tavishi. 2008. "Democracy and Dissent: Explaining Protest and State Response" (PhD dissertation, Emory University). Atlanta, GA.

Biddle, Sam. 2012. "Anonymous Explains CIA Takedown." *Gizmodo*, accessed February 11, 2012, http://gizmodo.com/5884346/anonymous-explains-cia-takedown.

Boehmke, Fred. 2008. "Plotfds: A Stata Utility for Plotting First Differences." Version: plotfds 1.1, updated December 16, 2008.

Bond, Doug, Joe Bond, Churl Oh, J. Craig Jenkins, and Charles Lewis Taylor. 2003. "Integrated Data for Events Analysis (IDEA): An Event Typology for Automated Events Data Development." *Journal of Peace Research* 40(6): 733–45.

Brecher, Aaron P. 2012. "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations." *Michigan Law Review* 111(3): 423–52.

Bronk, Chris. 2008. "Hacking the Nation-State: Security, Information Technology and Policies of Assurance." *Information Security Journal: A Global Perspective* 17(3): 132–42.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law* 17(2): 212–27.

Bueno de Mesquita, Ethan. 2005. "The Quality of Terror." *American Journal of Political Science* 49(3): 515–30.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

Chadwick, Andrew. 2006. *Internet Politics: States, Citizens, and New Communication Technologies*. Oxford: Oxford University Press.

Chinn, Menzie D., and Robert W. Fairlie. 2007. "The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration." *Oxford Economic Papers* 59(1): 16–44.

Cingranelli, David L., David L. Richards, and K. Chad Clay. 2014. The CIRI Human Rights Dataset. *CIRI Human Rights Data Project*, accessed April 14, 2014, www.humanrightsdata.com.

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins.

Collier, Paul, Lani Elliott, Havard Hegre, Anke Hoeffler, Marta Reynal-Querrol, and Nicholas Sambanis. 2003. *Breaking the Conflict Trap: Civil War and Development Policy*. Oxford: World Bank and Oxford University Press.

Collier, Paul, and Anke Hoeffler. 2004. "Greed and Grievance in Civil War." *Oxford Economic Papers* 56(4): 563–95.

Collier, Paul, and Nicholas Sambanis. 2002. "Understanding Civil War: A New Agenda." *Journal of Conflict Resolution* 46(1): 3–12.

Corrigall-Brown, Catherine. 2011. *Patterns of Protest: Trajectories of Participation in Social Movements*. Stanford: Stanford University Press.

Davenport, Christian. 2007. *State Repression and the Domestic Democratic Peace*. New York: Cambridge University Press.

Davenport, Christian, and David A. Armstrong. 2004. "Democracy and the Violation of Human Rights: A Statistical Analysis from 1976 to 1996." *American Journal of Political Science* 48(3): 538–54.

Denning, Dorothy. 2001. "Cyberwarriors: Activists and Terrorists Turn to Cyberspace." *Harvard International Review* 23(2): 70–75.

———. 2011. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell, 170–86. Hersey, PA: Information Science Reference.

Di Camillo, Federica, and Valérie Miranda. 2011. *Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward*. I. W. Papers, Instituto Affari Internazionali, 24. Rome, Italy.

Gakidou, Emmanuela, Krycia Cowling, Rafael Lozano, and Christopher J. Murray. 2010. "Increased Educational Attainment and Its Effect on Child Mortality in 175 Countries Between 1970 and 2009: A Systematic Analysis." *Lancet* 376(9745): 959–74.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. 2011. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political." *Technology and Society Magazine, IEEE* 30(1): 28–38.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38(2): 41–73.

Goth, Greg. 2007. "The Politics of DDoS Attacks." *Distributed Systems Online, IEEE* 8(8): 3–

Gurr, Ted Robert. 1970. *Why Men Rebel*. Princeton, NJ: Princeton University Press.

——— 2000. *People vs. States*. Washington, DC: United States Institute of Peace.

Gurr, Ted Robert, and William Moore. 1997. "Ethnopolitical Rebellion: A Cross-Sectional Analysis of the 1980s with Risk Assessments for the 1990s." *American Journal of Political Science* 41(4): 1079–1103.

Hashmi, Mohd Jameel, Manish Saxena, and Rajesh Saini. 2012. "Classification of DDoS Attacks and Their Defense Techniques Using Intrusion Prevention System." *International Journal of Computer Science and Communication Networks* 2(5): 607–14.

Hersher, Rebecca. 2015. "Meet Mafiaboy, The 'Bratty Kid' Who Took Down the Internet." National Public Radio, accessed October 1, 2015, http://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet.

Heston, Alan, Robert Summers, and Bettina Aten. 2012. Penn World Table Version 7.1, Center for International Comparisons of Production, Income, and Prices, at the University of Pennsylvania, July.

Holt, Thomas J. 2011. "Examining the Language of Carders." *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, 127–43. IGI Global.

Hoover, J. Nicholas. 2012. "Cyberattacks Becoming Top Terror Threat, FBI Says." *Information Week*, accessed February 1, 2012, http://www.informationweek.com/news/government/security/232600046.

Horton, Nicholas J., and Ken Kleinman. 2007. "Much Ado about Nothing: A Comparison of Missing Data Methods and Software to Fit Incomplete Data Regression Models." *American Statistician* 61(1): 79–90.

Jin, Shuyuan, and Daniel S. Yeung. 2004. "A Covariance Analysis Model for DDoS Attack Detection." 2004 IEEE International Conference on Communications, 4. Washington, DC: IEEE.

Jones, Andrew, and Gerald L. Kovacich. 2016. *Global Information Warfare: The New Digital Battlefield*. Boca Raton, FL: CRC Press.

Jordan, Tim, and Paul Taylor. 1998. "A Sociology of Hackers." *Sociological Review* 46(4): 757–80.

Kellner, Douglas. 2003. "Globalization, Technopolitics and Revolution." In *The Future of Revolutions*, edited by John Foran, 180–94. New York: Zedbooks.

King, Gary, James Honaker, Anne Joseph, and Kenneth Scheve. 2001. "Analyzing Incomplete Political Science Data: An Alternative Algorithm for Multiple Imputation." *American Political Science Review* 95(1): 49–69.

King, Gary, and Langche Zeng. 2001. "Logistic Regression in Rare Events Data." *Political Analysis* 9(2): 137–63.

Klesner, Joseph L. 2009. "Who Participates? Determinants of Political Action in Mexico." *Latin American Politics and Society* 51(2): 59–90.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

Krueger, Alan B., and David D. Laitin. 2008. "Kto Kogo? A Cross-Country Study of the Origins and Targets of Terrorism." In *Terrorism, Economic Development, and Political Openness*, edited by P. Keefer and N. Loayza, 148–73. New York: Cambridge University Press.

Krueger, Alan B., and Jitka Malečková. 2003. "Education, Poverty and Terrorism: Is There a Causal Connection?" *Journal of Economic Perspectives* 17(4): 119–44.

Lange, Matthew. 2011. *Educations in Ethnic Violence: Identity, Educational Bubbles, and Resource Mobilization*. New York: Cambridge University Press.

Lange, Matthew, and Andrew Dawson. 2010. "Education and Ethnic Violence: A Cross-National Time-Series Analysis." *Nationalism and Ethnic Politics* 16(2): 216–39.

Law, Terence K. T., John Lui, and David Ky Yau. 2005. "You Can Run, but You Can't Hide: An Effective Statistical Methodology to Trace Back DDoS Attackers." *Parallel and Distributed Systems, IEEE Transactions on* 16(9): 799–813.

Lee, Keunsoo, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, and Sehun Kim. 2008. "DDoS Attack Detection Method Using Cluster Analysis." *Expert Systems with Applications* 34(3): 1659–65.

Lesk, Michael. 2007. "The New Front Line: Estonia under Cyberassault." *Security and Privacy, IEEE* 5(4): 76–79.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corp.

Lichbach, Mark Irving. 1987. "Deterrence or Escalation? The Puzzle of Aggregate Studies of Repression and Dissent." *Journal of Conflict Resolution* 31(2): 266–97.

———. 1998. *The Rebel's Dilemma*. Ann Arbor: University of Michigan Press.

Lindsay, Jon R. 2014. "The Impact of China on Cybersecurity." *International Security* 39(3): 7–47.

Lu, ChiChao, WenYuan Jen, Weiping Chang, and Shihchieh Chou. 2006. "Cybercrime & Cybercriminals: An Overview of the Taiwan Experience." *Journal of Computers* 1(6): 11–18.

Machado, Fabiana, Carlos Scartascini, and Mariano Tommasi. 2011. "Political Institutions and Street Protests in Latin America." *Journal of Conflict Resolution* 55(3): 340–65.

Mansfield-Devine, Steve. 2011. "DDoS: Threats and Mitigation." *Network Security* 2011(12): 5–12.

Marshall, Monty G., Keith Jaggers, and Ted Robert Gurr. 2011. "*Polity IV Project: Political Regime Characteristics and Transitions, 1800–2010: Dataset Users' Manual*." College Park: University of Maryland.

Martinez, Lisa. 2008. "The Individual and Contextual Determinants of Protest Among Latinos." *Mobilization: An International Quarterly* 13(2): 189–204.

McCarthy, John D., and Mayer N. Zald. 1977. "Resource Mobilization and Social Movements: A Partial Theory." *American Journal of Sociology* 82(6): 1212–41.

Moore, Will H. 1995. "Rational Rebels: Overcoming the Free-Rider Problem." *Political Research Quarterly* 48(2): 417–54.

Murdie, Amanda, and Tavishi Bhasin. 2011. "Aiding and Abetting: Human Rights INGOs and Domestic Protest." *Journal of Conflict Resolution* 55(2): 163–91.

Narayan, V. 2013. "Most Online Criminals Are Educated Youths: Report." *Times of India*, accessed June 20, 2013, http://articles.timesofindia.indiatimes.com/2013-06-20/mumbai/40092858_1_cyber-crime-fraud-sexual-harassment.

Nazario, Jose. 2009. *Politically Motivated Denial of Service Attacks*. Cryptology and Information Security Series 3: 163–81. C. Czosseck and K. Geers. Fairfax, VA: IOS Press.

Neufeld, Derrick J. 2010. "Understanding Cybercrime." Paper presented at the System Sciences (HICSS), 43rd Hawaii International Conference Washington, DC: IEEE.

Norris, Pippa. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge, MA: Cambridge University Press.

Nye, Joseph. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly (Winter)* 5(4): 18–38.

Olzak, Susan. 1987. "Causes of Ethnic Conflict and Protest in Urban America, 1877–1889." *Social Science Research* 16(2): 185–210.

Pichardo Almanzar, Nelson A., and Cedric Herring. 2004. "Sacrificing for the Cause: Another Look at High-Risk/Cost Activism." *Race and Society* 7(2): 113–29.

Poe, Steven C., and C. Neal Tate. 1994. "Repression of Human Rights to Personal Integrity in the 1980s: A Global Analysis." *American Political Science Review* 88(4): 853–72.

Raghavan, S. V., and Edward Dawson, eds. 2011. *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection*. Berlin, Germany: Springer Science & Business Media.

Regan, Patrick M., and Daniel Norton. 2005. "Greed, Grievance, and Mobilization in Civil Wars." *Journal of Conflict Resolution* 49(3): 319–36.

Royston, Patrick. 2005. "Multiple Imputation of Missing Values: Update of Ice." *Stata Journal* 5(4): 527–36.

Sauter, Molly. 2014. *The Coming Swarm: DDoS Actions, Hactivism, and Civil Disobedience on the Internet*. New York: Bloomberg Academic.

Saxton, Gregory, and Michelle Benson. 2006. "Structure, Politics, and Action: An Integrated Model of Nationalist Protest and Rebellion." *Nationalism and Ethnic Politics* 12(2): 137–75.

Schofer, Evan, and Wesley Longhofer. 2011. "The Structural Sources of Association." *American Journal of Sociology* 117(2): 539–85.

Sherkat, Darren E., and T. Jean Blocker. 1994. "The Political Development of Sixties' Activists: Identifying the Influence of Class, Gender, and Socialization on Protest Participation." *Social Forces* 72(3): 821–42.

Sobek, David, M. Rodwan Abouharb, and Christopher G. Ingram. 2006. "The Human Rights Peace: How the Respect for Human Rights at Home Leads to Peace Abroad." *Journal of Politics* 68(3): 519–29.

Still, Brian. 2005. "Hacking for a Cause." *First Monday* 10(5). http://dx.doi.org/10.5210/fm.v10i9.1274.

Suler, John. 1997. "Psychological Dynamics of Online Synchronous Conversations in Text-Driven Chat Environments." *Psychology of Cyberspace*. http://users.rider.edu~suler/psycyber/texttalk.html

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018

Suler, John R., and Wende L. Phillips. 1998. "The Bad Boys of Cyberspace: Deviant Behavior in a Multimedia Chat Community." *CyberPsychology and Behavior* 1(3): 275–94.

Tarrow, Sidney. 1998. "Fishnets, Internets, and Catnets: Globalization and Transnational Collective Action." In *Challenging Authority: The Historical Study of Contentious Politics*, 228–44. Minneapolis: University of Minnesota.

Tarrow, Sidney, and Charles Tilly. 2007. "Contentious Politics and Social Movements." In *The Oxford Handbook of Comparative Politics*. Edited by Charles Boix and Susan Stokes, 435–60. Oxford: Oxford University Press.

Teorell, Jan, Nicholas Charron, Marcus Samanni, Sören Holmberg, and Bo Rothstein. 2011. The Quality of Government Dataset, version April 6. University of Gothenburg: Quality of Government Institute, accessed January 1, 2015, http://www.qog.pol.gu.se.

Tilly, Charles. 1978. *From Mobilization to Revolution*. Reading, MA: Addison-Wesley.

Valeriano, Brandon, and Ryan Maness. 2012. "The Fog of Cyberwar: Why the Threat Does Not Live Up to the Hype." *Foreign Affairs*, accessed January 1, 2015, http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar.

———. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11." *Journal of Peace Research* 51(3): 347–60.

———. 2015. *Cyber War versus Cyber Realities*. Oxford: Oxford University Press.

Vandevoort, John R. 1971. "Trade Secrets: Protecting a Very Special Property." *Business Lawyer* 26(3): 681–93.

Waldner, Lisa K. 2001. "Lesbian and Gay Political Activism: An Analysis of Variables Predicting Political Participation." *Research in Political Sociology* 9: 59–81.

Walsh, James I., and James A. Piazza. 2010. "Why Respecting Physical Integrity Rights Reduces Terrorism." *Comparative Political Studies* 43(5): 551–77.

Wheeler, David A., and Gregory N. Larsen. 2003. *Techniques for Cyberattack Attribution*. No. IDA-P-3792, 1–53. Alexandria, VA: Institute for Defense Analyses.

World Bank Group. 2012. *World Development Indicators 2012*. Washington, DC: World Bank Publications.

Xiang, Y., Y. Lin, W. L. Lei, and S. J. Huang. 2004. "Detecting DDOS attack based on network self-similarity." *IEE Proceedings - Communications* 151(3): 292.

Downloaded from https://academic.oup.com/jogss/article-abstract/1/3/235/2579752 by American Univ WCL user on 05 December 2018