

At Home and Abroad: The Use of Denial-of- service Attacks during Elections in Nondemocratic Regimes

Journal of Conflict Resolution

1-29

© The Author(s) 2019



Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/0022002719861676

journals.sagepub.com/home/jcr

Philipp M. Lutscher¹ , Nils B. Weidmann¹ ,
Margaret E. Roberts², Mattijs Jonker³, Alistair King⁴,
and Alberto Dainotti⁴

Abstract

In this article, we study the political use of denial-of-service (DoS) attacks, a particular form of cyberattack that disables web services by flooding them with high levels of data traffic. We argue that websites in nondemocratic regimes should be especially prone to this type of attack, particularly around political focal points such as elections. This is due to two mechanisms: governments employ DoS attacks to censor regime-threatening information, while at the same time, activists use DoS attacks as a tool to publicly undermine the government's authority. We analyze these mechanisms by relying on measurements of DoS attacks based on large-scale Internet traffic data. Our results show that in authoritarian countries, elections indeed increase the number of DoS attacks. However, these attacks do not seem to be directed primarily against the country itself but rather against other states that serve as hosts for news websites from this country.

¹Department of Politics and Public Administration, University of Konstanz, Konstanz, Germany

²Department of Political Science, University of California, San Diego, CA, USA

³Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, The Netherlands

⁴Center for Applied Internet Data Analysis, San Diego Supercomputer Center, University of California, San Diego, CA, USA

Corresponding Author:

Nils B. Weidmann, Department of Politics and Public Administration, University of Konstanz, 78457 Konstanz, Germany.

Email: nils.weidmann@uni-konstanz.de

Keywords

cyberattacks, autocracy, Internet measurement, digital politics

As the importance and penetration of information and communication technology (ICT) is rapidly increasing worldwide, it is not surprising that attacks on this infrastructure have also increased steadily. One of the most common type of cyberattacks are denial-of-service (DoS) attacks, which aim to interrupt the operation of servers and websites by flooding them with data traffic. Many, if not most, of these attacks have criminal intentions, for example, targeting companies for ransom. However, DoS attacks are also used for political purposes. For instance, at the time of the Russian election on December 4, 2011, many independent Russian news agencies and opposition websites encountered DoS attacks when they published articles about potential election fraud. At the same time, there were reports of DoS attacks on government election bodies by activist groups, presumably as an attempt to protest against election irregularities (Roberts and Etling 2011). These examples suggest that DoS attacks can indeed be employed for political purposes, either as a tool of censorship to silence the opposition or as a weapon of the weak against a mighty government. Is this a systematic pattern? What types of political regimes are particularly prone to this type of digital attack? And how do political events affect their occurrence?

So far, little is known about the political use of DoS attacks. Some work in political science studies cyberattacks (of which DoS attacks only constitute one example) in interstate rivalries (Valeriano and Maness 2014). Asal et al. (2016) explore country-specific factors that lead to an increased frequency of politically motivated DoS attacks. Most recently, Kostyuk and Zhukov (2019) investigate the interplay between DoS attacks and battlefield events in Ukraine and Syria. While this work tells us something about the international drivers of DoS attacks, we have yet to examine the use of these attacks for domestic political purposes. As suggested by our introductory examples (and several others we describe below), DoS attacks have the potential to become a digital weapon of choice for governments but also opposition activists. Moreover, existing research has been limited to aggregated country-level comparisons (which make it difficult to trace the dynamic relationship between political events and the frequency of attacks) or studies with a country-specific focus (which preclude insights into other cases beyond the one studied).

Our approach in this article is different. We analyze the use of DoS attacks for domestic political purposes across almost all political regimes worldwide and trace their occurrence at a high temporal resolution. In doing so, our focus is on election periods as one of the main focal points of political contention. There is considerable anecdotal evidence that cyberattacks occur frequently during election periods, especially in nondemocratic regimes (Freedom House 2017). Governments in these countries have high incentives to use DoS attacks to censor regime-threatening

websites, while for activists DoS attacks are a low-cost alternative to show their disagreement during contentious periods. For our empirical investigation, we rely on a data set of DoS attacks derived from Internet traffic observations on the network infrastructure. In contrast to media-based data on cyberattacks, we avoid reporting biases of different kinds, such as attacks that go unreported if they are not successful or if they target nongovernmental groups (Hardy et al. 2014, 1). This attack data set is one of the most comprehensive and fine-grained data source on DoS attacks available, allowing us to determine the exact date and country of the attacked server and even capture attack attempts.

Using this data set, we conduct a statistical analysis on a sample of 186 countries with elections, using weekly observations from March 2008 through December 2016. Our results show only limited evidence for an increase of DoS attacks against servers within more authoritarian countries during time periods around elections. However, since opposition groups and media outlets frequently host their websites abroad, we use data on where each country's news media is hosted to measure whether the election prompted attacks on domestic media websites hosted internationally. Here, we find a pronounced and robust increase in the frequency of DoS attacks during election periods in more authoritarian regimes. This finding indicates that authoritarian regimes are likely using DoS attacks during election periods and other contentious periods to censor domestic media websites that are hosted abroad, taking advantage of the deniability and flexibility of DoS attacks to export censorship beyond their borders.

Related Literature and Theoretical Argument

While many scholars have praised the Internet as "liberation technology" for citizens in authoritarian regimes and underrepresented groups (e.g., Diamond 2010), others have also emphasized the enhanced possibilities for (authoritarian) governments to censor and repress (e.g., Morozov 2011). The more recent literature has moved beyond this simplified distinction and emphasizes that the Internet can play both roles and that they are not mutually exclusive (e.g., Roberts 2018; Dragu and Lupu 2017; Tucker et al. 2017). DoS attacks reflect this dual character of modern ICT: governments or state-near groups can use them to censor and temporarily disable unwanted outlets, while activists can use DoS attacks as a new tool to attack state servers in times of political turmoil. In the following, we discuss these two uses of DoS attacks, before arguing that both uses imply that DoS attacks should increase during election periods in more authoritarian countries.

A Tool for Censorship

According to Freedom House (2016), more than 35 percent of the world's Internet population lives in regimes where the Internet is actively censored and online activists are harassed and/or surveilled.¹ There are many ways to manipulate content on

the Internet. For example, governments pass legislation that restrict access to certain unwanted domestic websites and servers (Deibert and Rohozinski 2010) or apply pressure on the Internet service provider (ISP) to delete content (King, Pan, and Roberts 2013). Other strategies are to harass online bloggers and discredit them in social networks (Pearce and Kendzior 2012; MacKinnon 2013) or use the Internet and social media for pro-government propaganda (Gunitsky 2015; MacKinnon 2013; King, Pan, and Roberts 2017).

While these methods of censorship may work for domestic websites, controlling websites hosted abroad is more difficult since the government does not have the jurisdiction to pressure international companies into removing content. Sophisticated regimes such as China and Saudi Arabia can block outside websites with firewalls, preventing citizens from accessing selected websites abroad from domestic Internet addresses (Boas 2006; MacKinnon 2013). Even though firewalls can be evaded, often citizens are not sufficiently sophisticated or interested enough to route around them (Hobbs and Roberts 2018; Chen and Yang 2019). A more drastic tool for controlling citizen access to foreign content that also is simpler for less sophisticated regimes is the temporary complete shutdown of the national Internet, for example, the Egyptian and Libyan Internet network shutdown that occurred during the Arab Spring (Dainotti et al. 2014; Hassanpour 2014).²

DoS attacks can be used as another means of both domestic and international censorship; however, they have received little attention in the literature so far. The main effect of DoS attacks is to temporally restrict access to specific websites by targeting the hosting server. Conventional wisdom suggests that the political targets of DoS attacks are likely to be online newspapers or TV stations reporting on government-threatening news or opposition websites and regime-critical NGOs in general. In addition to temporarily shutting down a website, DoS attacks can function as a repressive signal to the respective outlet, which might consider self-censoring in the future. While there is some anecdotal evidence that DoS attacks were also used to target ISPs in order to restrict the access to the Internet more generally (Villeneuve and Crete-Nishihata 2012), this use is relatively rarer than targeted attacks on specific websites.

The fact that DoS attacks are not restricted to the censoring of servers within a country but are able to target servers abroad may be especially helpful for nondemocratic regimes since many opposition websites, news portals, and blogs are often hosted abroad to bypass direct national Internet control. Many countries also do not have the necessary network infrastructure to host servers reliably, which is another reason why websites can rely on hosting providers abroad. While the blocking of foreign websites is also possible with other means (e.g., Domain Name System [DNS] filtering or countrywide firewalls), only technologically sophisticated authoritarian countries are able to employ these tools and these methods only restrict the access for domestic users. In contrast, DoS attacks are relatively low cost, easy to employ, and are able to temporally disable access for the domestic population *and* international observers. According to a report about the Russian online black market,

it is possible to buy DoS attacks starting at 70 US\$ per day (Goncharov 2012). In addition, DoS attacks are very precise and can be used to target particular websites and servers. Thus, DoS attacks are much cheaper than inducing a complete network outage, which is accompanied by high economic costs and international attention. Lastly, while the owners of a website may realize they are being attacked, DoS attacks are not obvious to website users and difficult to trace to the source of the attack (Deibert and Rohozinski 2010). This means it is possible for governments to simply deny responsibility for these attacks and avoid national and international reputational costs.

Overall, these features suggest that DoS attacks are not only attractive for clearly nondemocratic regimes but also for semi-democratic governments that want to tilt the political playing field in their favor. Many of these governments are unable to opt for more drastic means of censorship (because they do not have the technical capabilities) or are unwilling to do so (because they want to be perceived as democratic). Instead, they rather use more subtle censoring tools. DoS attacks may be an attractive alternative to censor selectively government-threatening websites, while also allowing these governments the cover of plausible deniability.

Anecdotal evidence suggests that governments use DoS attacks during politically contentious times or outsource them to pro-regime groups or state-near hackers (Deibert et al. 2008; Deibert and Rohozinski 2010; Zuckerman et al. 2010). For example, before the Russian election in late 2007, the website of the opposition politician and famous chess player Gary Kasparov was targeted by a DoS attack (Nazario 2009). Four years later, similar DoS attacks targeted many independent newspapers and blogs, as well as Internet TV stations, before and on the Russian election day, December 4, 2011 (Jagannathan 2012). Some investigations highlight that many of these attacks were ordered by the Russian government and conducted by the pro-Kremlin group "Nashi" or loyal hacker groups using botnets (Carr 2011). Beyond Russia, there are also widespread reports of DoS attacks on Burmese opposition websites during important events such as elections and protest anniversaries, where the opposition websites were targeted, even though their servers were hosted abroad (Villeneuve and Crete-Nishihata 2012). One of the largest DoS attacks to date occurred during the Hong Kong protests in 2014 and was directed against the independent news and opposition websites *Apple Daily* and *PopVote* (Olson 2014). Here, Chinese authorities were likely behind these attacks, in an attempt to still censor these outlets even though they had no direct control over the websites hosting providers. Another example of a country-sponsored use of DoS was the large-scale attack on the Chinese censorship circumvention website Greatfire.org, which even affected the global collaboration platform Github in 2015. A report by Citizenlab presented evidence that the Chinese government was behind these DoS attacks, calling the attack tool "China's Great Cannon" due to its impressive capabilities (Marczak et al. 2015).

Apart from these cases, there are several media reports on attacks against independent news websites in Belarus, Azerbaijan, and other post-Soviet states, as well

as in countries such as Turkey or Venezuela. These attacks happened primarily when websites reported on electoral fraud, protests, or repressive government actions (Cardenas 2017; Karnej and Whitmore 2008; Qurium 2017; The Turkish Newswire 2014; Yildirim 2016). While all of these examples highlight that government actors are most likely to be the initiators of DoS attacks on critical and threatening websites, it is oftentimes not possible to attribute DoS attacks to specific actors. As shown in the case of the Russo-Georgian war in 2008, it may also be that patriot hacking groups (alone or complementary) use DoS attacks as they disagree with specific content and want to support their country out of patriot sentiments (Deibert, Rohozinski, and Crete-Nishihata 2012).

A Tool for Contention

While as a powerful tool in the hands of governments, DoS attacks can also be used against them. Modern information and communication technologies have extended the contentious action repertoire for social movements and groups (Van Laer and Van Aelst 2010). While there is extensive work on how the Internet helps groups and social movements mobilize (e.g., Diamond 2010; Enikolopov, Makarin, and Petrova 2018; Little 2016), less research is concerned with exclusively digital forms of contention. DoS attacks are useful for activists groups because they can act as a form of protest against governments, punish governments for their actions, and throttle communication via government websites from the government to the broader population. Research in sociology and anthropology discusses the use of DoS attacks as a kind of protest for online activists (Coleman 2014; Jordan 2002; Milan 2015; Sauter 2014; Wong and Brown 2013). Sauter (2014) argues that DoS "actions" conducted by activists should be perceived as a form of legitimate protest and civil disobedience. For example, in 2011, when the online collective *Anonymous* started with its "Operation Payback" against PayPal after the company refused to forward payments to WikiLeaks, the group used DoS attacks to temporarily shut down PayPal servers. For this operation, *Anonymous* distributed a custom-designed software called the "Low Orbit Ion Cannon," which turns users' computers into DoS attackers (Coleman 2014).

It is not surprising that DoS attacks are often used by activists, since there are several advantages of DoS attacks for these actors. First, attackers do not have to be physically present and can start attacks from all around the world. Second, and in contrast to other forms of hacking, DoS attacks require very few technical skills but are still a powerful and visible tool to show disagreement. If, for example, government websites, mail servers, or official news agency of a country is not accessible for several hours, this is likely to be noticed by regime officials, citizens, and press agencies. Thus, these attacks make the regime look vulnerable or weak domestically and internationally. Furthermore, depending on the targeted website, communication and information flows by the regime to the broader population can be temporally distorted. Third, DoS attacks can come with relatively low costs with regard to

possible legal or repressive consequences, as they are hard to trace back. This makes them particularly attractive for activists in more authoritarian regimes as a low-cost alternative to show disagreement (Dolata and Schrape 2016; Milan 2015, 551-52). Nevertheless, some basic understanding of Internet technology is necessary for this. For example, many activists who used the "Low Orbit Ion Cannon" software for collective DoS attacks against PayPal and other websites in 2011 were later prosecuted because the program did not hide the attackers' Internet addresses (Olson 2013). Therefore, while many of the abovementioned advantages are true, activists nevertheless need a basic understanding of Internet communication in order to use these attacks without being traceable.

Anecdotal evidence and studies about *Anonymous* and others show that their political actions have become more salient in recent years and that they mount attacks primarily as a reaction to real-world political events (Coleman 2014). For example, the Iranian election fraud in June 2009 led not only to widespread physical protests but also to domestic and international activists using DoS attacks to protest the Iranian regime online. To show their disagreement, activists launched attacks against the website of President Ahmadinejad and other government institutions, including the official Iranian news agency (Beyer 2014). In 2011, *Anonymous* also supported the widespread antiregime protests against authoritarian regimes in the Middle East and North Africa (MENA) region with attacks against government websites (Coleman 2014; Olson 2013).

A more systematic study finds that on a yearly aggregate level, popular unrest and repression are a country's best predictors for being targeted by DoS attacks (Asal et al. 2016). Although this finding is based on media-reported attacks and therefore might only reflect high-profile attacks, it highlights that activists are more likely to mount DoS attacks in response to real-world political events but also in response to systematic opposition harassment by a regime (Coleman 2014; Milan 2015; Olson 2013; Sauter 2014). For example, the increased repression against Tunisian protesters in January 2011 triggered an outcry in the cyberspace. Shortly after, *Anonymous* started DoS attacks against the Tunisian regime in order to increase international attention (Coleman 2014, 152-53). Likewise, when during Iran's 2009 election the regime responded with repression, DoS attacks became a useful tool to complement ordinary protest (Beyer 2014). Supporting this finding, a survey by Holt et al. (2017) shows that the willingness to participate in real-world protests against governments and use cyberattacks against them is highly correlated.

Election Periods, Authoritarianism, and DoS Attacks

The previous discussion highlights that DoS attacks can be used for political purposes by governments and activists alike. If this is true, the intensity of DoS attacks should be higher in time periods of political contention. Elections constitute political focal points during which political confrontation is typically high, and this holds across democratic and autocratic regimes. While elections are obviously a core

feature of the former, there are only very few autocratic regimes that do not hold elections. Existing work has argued that elections are held by authoritarian regimes to co-opt elites (Gandhi and Lust-Okar 2009), show regime strength (Magaloni 2008), receive information about their popularity (Little 2012), and gain legitimacy (Schedler 2013). At the same time, elections constitute some of the most important focal points for antiregime activities and political unrest within nondemocratic regimes (Lindberg 2009; Tucker 2007; Shirah 2016; Schedler 2013; Knutsen, Nygård, and Wig 2017). Following the outlined motivations to use DoS attacks, we should thus expect that DoS attacks are systematically launched during election periods in more authoritarian regimes.

Incumbent governments have strong incentives to minimize the risk of popular unrest during election periods. Whereas democratic regimes are constrained in their ability to use censorship, more authoritarian regimes may seek to minimize unrest by censoring politically sensitive information. DoS attacks can be used to attack opposition and news websites in order to censor accusations of election fraud or calls for collective action. Governments can even engage in preventive censorship and attempt to shut down news outlets they expect to be critical of the regime. For instance, before the Russian elections in 2011, independent news websites were targeted by DoS attacks before the election (Jagannathan 2012). Other examples of DoS attacks during authoritarian elections include attacks during the election in Turkey in 2015, Russia in 2007, or Malaysia in 2011 (Freedom House 2017; Nazario 2009; The Australian 2011).

Activist groups should also have higher incentives to use DoS attacks in more authoritarian contexts during election periods. Domestic and international activists might target government and election-related websites to protest against electoral fraud and other repressive government actions as well as support protests on the ground. Whereas democracies have multiple channels for the public to express discontent, channels of contention are limited in more authoritarian regimes, and DoS attacks might be a viable alternative to express dissatisfaction. Anecdotal evidence for attacks due to these motivations were DoS attacks on government websites around the elections in Iran in 2009, Russia in 2011, or Turkey in 2011 (Beyer 2014; Butler 2011; Roberts and Etling 2011). Thus, our first hypothesis is that:

Hypothesis 1: The frequency of DoS attacks against domestic servers increases during election periods. This effect should be more pronounced the more authoritarian a country is.

This increase of attacks on the country can be either caused by activists targeting a country's government servers and websites and/or attacks on opposition and news websites that are hosted within the country with the aim to silence them. In addition to domestic attacks, many opposition groups and newspapers (unlike government websites) host their websites abroad. If governments use DoS attacks to censor these

servers outside their jurisdictions, we should observe that election periods in less democratic regimes should also increase the number of DoS attacks on the countries where these servers are located. Therefore, we expect that:

Hypothesis 2: The frequency of DoS attacks against countries that host domestic media websites increases during election periods. Again, this effect should be more pronounced the more authoritarian a country is.

Lastly, we can assume that the proximity of election is related to the level of political tension, which should increase the closer we get to an election. This should lead to more efforts of Internet censorship and online protesting shortly before, during, and after the election day (Schedler 2013). Thus, we expect that:

Hypothesis 3: The increase in (domestic and foreign) DoS attacks becomes stronger the closer the respective country is to an election.

New Data to Measure DoS Attacks

For our analysis, we require fine-grained, systematically measured data on DoS attacks. Most of the existing research relies on English language newspaper articles only to code politically motivated DoS attacks (e.g., Asal et al. 2016; Valeriano and Maness 2014).³ The reliance on newspaper articles can be problematic due to potential reporting bias: First, only interesting attacks (e.g., those that are large and successful attacks) may be reported by the media, especially when the affected country is already in the center of attention (cf. Earl et al. 2004). Second, there is a clear bias with regard to English-speaking countries and attacks on other countries, particularly nondemocratic ones, are unlikely to be covered comprehensively. Lastly, Hardy et al. (2014, 1) highlight that especially attacks on human rights organization and civil society actors are less frequently reported, which might underestimate the use of DoS attacks as a convenient censoring tool for governments and state-near groups.

To remedy this issue, we rely on high-resolution attack estimates provided by the Center of Applied Data Analysis (CAIDA 2016) at the University of California, San Diego from 2008 to 2016 (Jonker et al. 2017). Our data capture one of the most frequently used types of DoS attacks, so-called randomly spoofed attacks. “Spoofing” means that attackers craft their flood of requests to the target such that it appears to originate from one or several *fake* (i.e., not corresponding to the machine(s) executing the attack) Internet addresses. This helps them hide their true identities but also makes it more difficult for a victim to fend off an attack by simply blocking incoming traffic from a particular address (Zargar, Joshi, and Tipper 2013). Since the targeted server responds to the fake addresses, CAIDA monitors these responses through their network telescope and can detect them if the fake address falls within the telescope’s large address space (approximately 1/256th of all IPv4 Internet addresses). For more details on this estimation method, please refer to Moore et al. (2006).

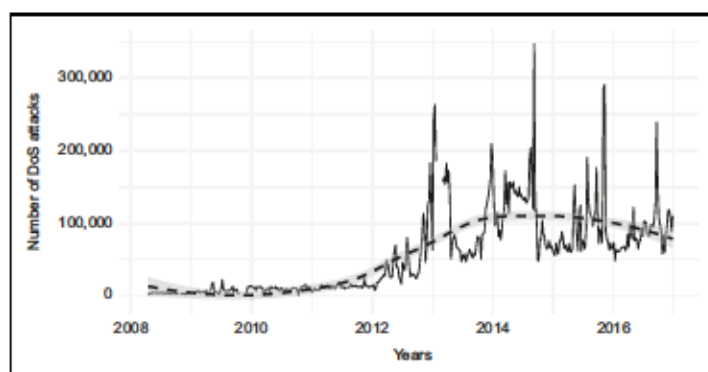


Figure 1. Number of denial-of-service attacks 2008 to 2016 over time (in countries with elections). The dashed line shows the smoothed trend.

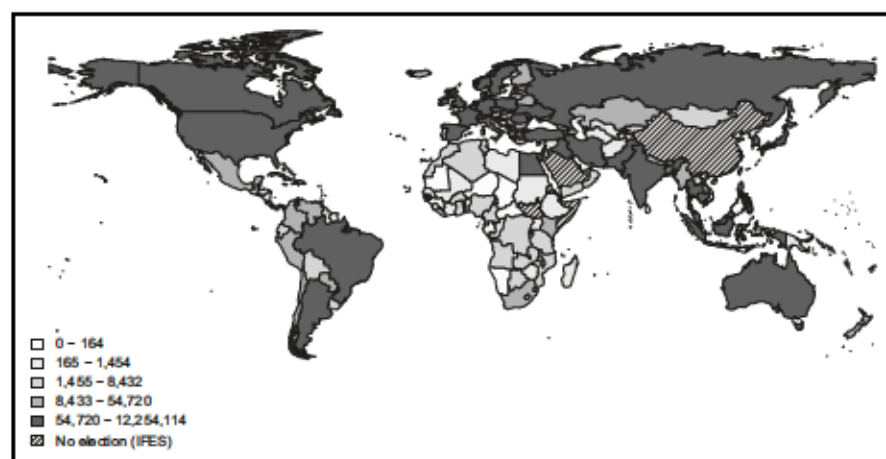


Figure 2. Number of denial-of-service attacks 2008 to 2016 in countries with elections. Country borders based on Weidmann, Kuse, and Gleditsch (2010).

Overall, our data record more than twenty-two million attacks during this period. Figure 1 illustrates the temporal development of DoS attacks and highlights a worldwide steady increase, especially from the year 2012 onward. This reflects an increase in the number of Internet devices (potential targets) but also that attacks have become stronger and more frequent in recent years. Figure 2 shows the relative difference between the absolute number of attacks between countries from 2008 to 2016. The figure points to large differences between countries: whereas larger and more developed countries such as the United States and Russia experienced the most DoS attacks, fewer attacks were conducted against servers in African countries.

There are some significant advantages of our approach, since our data do not rely on media-derived information about DoS attacks. Foremost, our data are not prone to media bias. Most importantly for our research question, this means that media attention, which is likely to be higher during election periods, does not influence our measurement. Second, our data even include the smallest DoS attacks and also attack attempts. Even if the target website is not shut down completely, the attack will still appear within the data. Additionally, we have information about the attack strength and duration, exact time of the attack, and even the targeted IP address, which we use to infer the geographic location of the attacked server. However, there are also some limitations in our data source. For once, our assessment of attacks might be described as conservative because we are only capturing randomly spoofed DoS attacks, which only constitute a subset of all attacks. Nevertheless, recent studies show that spoofed DoS attacks are extremely popular and comparable in numbers to reflection attacks (another popular class of DoS techniques). Due to the fact that both types of DoS attacks display comparable patterns (see Jonker et al. 2017, 105), our data are a good approximation of the overall level of DoS attacks on a country at a specific point in time. Furthermore, there is evidence that both attack types are sometimes even used in conjunction (Internet Society 2015; Jonker et al. 2017). Another limitation is that due to the fake addresses used by attackers, we cannot infer the identity of the attacker or even his or her country of origin. Our analysis therefore focuses exclusively on the country of the target website.

Research Design

In this section, we describe how we aim to test our theoretical expectations using panel data of 186 countries from March 2008 through December 2016. We use one-week granularity as a good trade-off between temporal accuracy and potential problems due to temporal dependence. Our analysis includes all regimes that held at least one national election during the period of study, as recorded in the ElectionGuide database (International Foundation for Electoral Systems [IFES] ElectionGuide 2017).⁴ The focus on election periods has the empirical advantage that election dates are normally determined well in advance. Hence, DoS attacks do not influence election periods and we avoid problems of reverse causality. In the following, we describe the variables included in our analysis and the research design we employ. Summary statistics for all variables are available in Table A.1 in the Appendix.

Dependent Variables

To construct our dependent variables, we use CAIDA's data set described in the previous section (CAIDA 2016; Jonker et al. 2017). Our first main variable of interest is the number of spoofed DoS attacks per week and country. This variable only measures the overall level of attacks on domestic servers in the respective country, which means that it includes all sorts of attacks (nonpolitical vs. political,

the latter against state as well as nonstate actors). Since we cannot distinguish between political and nonpolitical targets in our data, our later statistical analysis focuses on deviations from the overall attack level that can be attributed to elections, assuming that additional DoS attacks during election periods have some political motivation.

Second, as argued above, many potential opposition groups and newspapers host their websites abroad to bypass direct government control and/or due to the better network infrastructure in more developed countries. In order to test our second hypothesis, we therefore construct a spatially lagged attack variable that estimates the number of attacks in those countries where a large number of a given country's websites are hosted. To create this spatial lag for our second dependent variable, we rely on information from www.abyznewslinks.com, which to our knowledge is the only comprehensive listing of news websites worldwide. For countries with very large numbers of news websites (Brazil, Canada, US, UK, Germany, India, and Australia), the data set distinguishes between national and regional sites, and we only use the former. From the news website data set, we use DNS lookups to identify where each website is hosted (van Rijswijk-Deij et al. 2016). We then compute the sum of the attacks in all other countries weighted by the share of the target country's national news websites they host.⁵ The indicator is calculated as follows:

$$DoS_foreign_hosts_{it} = \sum_{j=1}^{N-i} p_{ij} \times DoS_{jt}, \quad (1)$$

where $N - i$ denotes all countries except country i , p_{ij} refers to the proportion of hosted websites of country i in country j , and DoS_{jt} is the number of DoS attacks on country j at time t . While we measure the web hosting relationships between countries using news websites only, it is very likely that other opposition and regime-critical websites follow a similar relationship, whereas government websites are rather hosted within the country. To reiterate the point from above, this variable measures again the overall level of DoS attacks, in this case, on foreign hosts. Thus, we can still not distinguish between political and nonpolitical attacks (a task we attempt to solve in our later statistical approach). One issue with this approach is that we were only able to look up IP addresses for news websites in November 2017. Websites can change their hosting servers and potentially their hosting country. Thus, to minimize error in this variable, we restrict the second analysis to the years 2014 to 2016. We believe that the restriction to three years ensures that the dependent variable is accurate, while still providing enough data to assess the relationship between attacks and elections. We conduct a number of additional analysis to check the robustness of our findings for this second dependent variable.

Explanatory Variables

For our explanatory variable *election period*, we use information about national election dates from ElectionGuide, including national parliament, senate, and

presidential elections (IFES ElectionGuide 2017). Our independent variable of interest is a dummy variable that indicates whether a given week is an election week or is within three weeks before or after the election. We consider three weeks as a good trade-off to capture the increased political tension around elections and to create enough variation in our variable of interest. In further tests, we check the robustness of our findings to different definitions of the election period dummy.

As per our hypotheses, we expect the relationship between elections and DoS attacks to hold primarily in authoritarian regimes. To identify these regimes, we use an index for electoral democracy created by the V-Dem project (Coppedge et al. 2016). This index measures electoral competitiveness, whether political and civil society organization can engage freely and whether elections are free of systematic irregularities. Furthermore, the index considers freedom of expression and independent media between elections but does not include any measure of Internet censorship. To ease the interpretation of our results, this electoral democracy index is inverted, ranging from 0 (full democracy) to 1 (full autocracy). We refer to this index as autocracy index. In later sensitivity tests, we also run the same analyses using the Polity measure (Marshall and Jaggers 2016), although this index is not available for the entire period of our analysis.

Method

We employ a panel data approach and include country \times year fixed effects. Using this specification, we not only control for time-invariant country-specific factors that explain the average number of attacks on a country, but we also take annual country-specific time trends into consideration. Therefore, this approach nets out time-variant yearly developments in a country's Internet penetration, level of censorship, and so on, that might increase or decrease the average number of attacks on domestic and foreign servers and only considers variation within each country-year. A higher number of DoS attacks during election periods (compared to the country-year average) indicate that some of them are politically motivated, assuming that the level of nonpolitically motivated attacks does not systematically change at the same time. Due to the skewed distribution of our attack variables, our main model specification is a log-linear model with an interaction between election period and the autocracy index. The model is specified as follows:

$$\ln(\text{DoS}_{i,t} + 1) = \beta_1 \text{election}_{i,t} + \beta_2 (\text{election}_{i,t} \times \text{autocracy}_{i,t}) + \delta_{i,t} + \epsilon_{i,t} \quad (2)$$

where $\delta_{i,t}$ includes the country \times year fixed effects and $\epsilon_{i,t}$ represents the error term. Due to the fact that our fixed effects are introduced at the country-year level, the main effect for the autocracy index is captured by these as this variable does not vary on the country-year level. Furthermore, we account for serial correlation and heteroscedasticity by using Newey–West corrected standard errors clustered at the country-year level.⁶

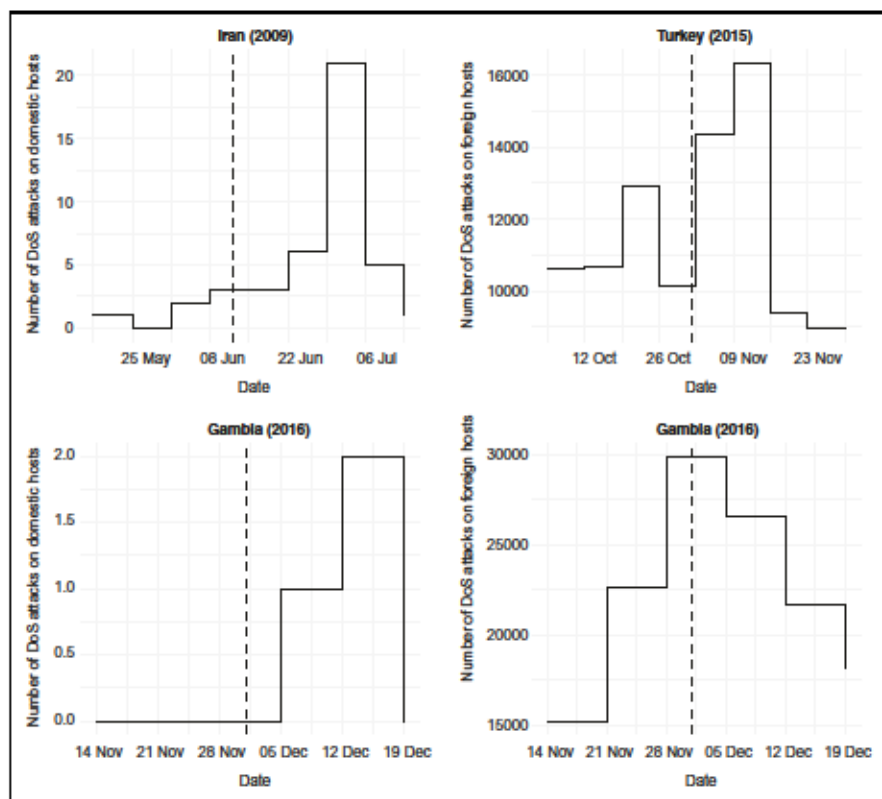


Figure 3. Denial-of-service attacks during election periods in Iran (2009), Turkey (2015), and Gambia (2016). The dashed black vertical line represents the election date, whereas the solid line illustrates the development of DoS attacks in the respective weeks.

Analysis

In this section, we first examine the relationship between election periods and the number of DoS attacks using some illustrative examples as well as bivariate comparisons. Later, we present the main results of our statistical analysis as well as the results of several sensitivity and robustness tests.

Descriptive Evidence

Figure 3 provides a case example for the relationship between election periods and DoS attacks within authoritarian regimes. The left panel illustrates the development of DoS attacks against Iran in 2009 and highlights an increase in attacks after the election and the eruption of antiregime protests. Anecdotal evidence emphasizes that mainly activists were responsible for the attacks, targeting government websites in

Table 1. Average Number of Denial-of-service Attacks per Week on the Country and on Foreign Hosts.

	Attacks on Domestic Hosts (2008–2016)		Attacks on Foreign Hosts (2014–2016)	
	Democracy	Autocracy	Democracy	Autocracy
Elections	557.99	106.32	18788.51	22304.41
No Elections	502.28	96.63	21699.88	21527.86

order to protest against election fraud and to support antiregime activities on the ground (Beyer 2014). The right panel shows the development of DoS attacks on foreign hosts in the case of Turkey in 2015 and highlights an increase of DoS attacks before as well as just after the election. This time, anecdotal evidence highlights attacks on critical newspapers, for example, the (now dissolved) Cihan News Agency that was hit by DoS attacks during the November 1 election (Freedom House 2017). Another recent example of a rise in DoS attacks during an election period could be observed in Gambia in the year 2016. Here, the government heavily restricted the influence of independent media and social media and even blocked Internet access just before the election. The bottom panel in Figure 3 shows that we can see both, an increase of attacks on the country (left panel) and on foreign hosts (right panel). While not all of the attacks on foreign hosts are related to attacks on critical news outlets, these patterns are consistent with the motivation of the Gambian government trying to reduce the impact of independent media.

To more generally investigate the relationship between elections, DoS attacks, and the level of autocracy, we simply compare the level of DoS attacks per week during election periods with nonelection weeks in democracies and autocracies. As the autocracy index has no qualitative threshold, we set 0.5 as a threshold to classify countries in democratic (autocracy index < 0.5) or authoritarian regimes (autocracy index \geq 0.5).⁷ Table 1 shows some first differences between democratic and authoritarian regimes. In general, with regard to DoS attacks on domestic hosts, the table reveals that democracies are far more often hit by DoS attacks. This is not surprising, since these countries are, on average, more developed, possess a more extensive IT infrastructure, and are thus much more likely to suffer from cyberattacks. Second, the table also shows that election periods slightly increase the number of DoS attacks, but counter to our expectation, this occurs in autocracies as well as democracies. For the attacks on foreign hosts (2014–2016), we see very similar numbers outside election periods for both regime types (lower row). This number, however, decreases in election periods for democracies but increases for autocracies. In sum, our descriptive analysis provides only limited support for our theoretical expectation that DoS attacks are more frequently used during election periods in more authoritarian countries. However, so far we have only conducted simple bivariate

Table 2. Relationship between Election Periods, Level of Autocracy and Denial-of-service Attacks (Country/Week).

	Model 1	Model 2	Model 3	Model 4
	Domestic	Domestic	Foreign	Foreign
Election period	-.032* (.014)	-.039 (.030)	-.020 (.012)	-.096*** (.026)
Election period \times autocracy index		.036 (.065)		.230*** (.055)
Country \times year fixed effects	Yes	Yes	Yes	Yes
Num. obs.	81,305	70,817	28,175	24,503

Note: Robust standard errors clustered at the country-year level in parentheses.

*** $p < .001$.

** $p < .01$.

* $p < .05$.

comparisons, without taking into account the continuous character of our autocracy index, country-specific developments, and alternative factors. Therefore, the next section introduces our multivariate statistical models that remedy these shortcomings.

Main Models

Our main statistical models are reported in Table 2. The models 1 and 2 use the logged number of attacks on the country, and models 3 and 4 use the logged number of attacks on foreign hosts. Models 1 and 3 only include the (noninteracted) independent variable. Here, our results even highlight a (weak) negative relationship between election periods and DoS attacks. Models 2 and 4 include interaction effects with our autocracy index to test whether the effect of elections on DoS attacks is moderated by the level of autocracy.

To better illustrate the estimated relationships of the interaction models, Figure 4 shows the estimated coefficient for elections periods conditional on the autocracy index. As already stated above, the models do not include the main effect for the autocracy index as this variable is not varying on the year level and hence captured by the country \times year fixed effects. The left panel highlights the systematic relationship between the election periods and DoS attacks depending on the level of autocracy. In fact, the overall relationship remains negative (but displays overall high levels of uncertainty especially for very authoritarian countries). Thus, we do not find support for Hypothesis 1 that expects a stronger positive effect of election periods on DoS attacks on the country for more authoritarian regimes, and the results suggest that government servers and/or opposition servers hosted within the country

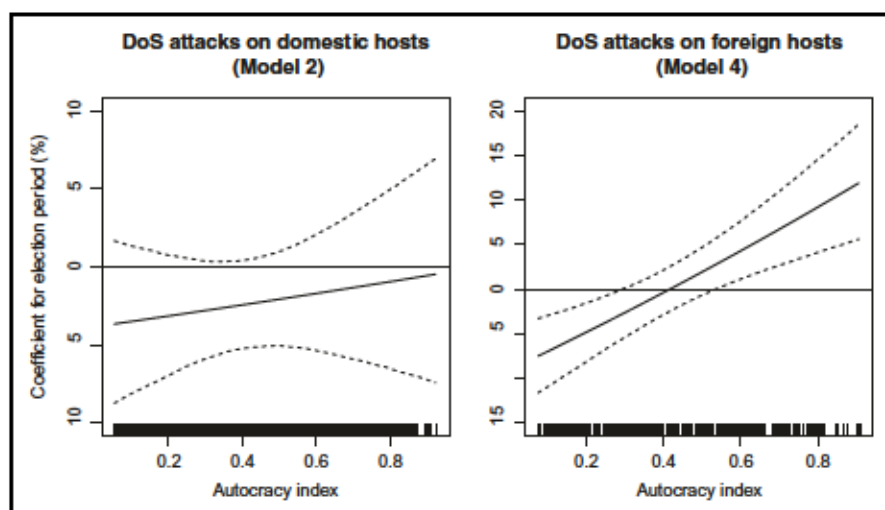


Figure 4. Effect of election period on DoS attacks, dependent on the level of autocracy; 95 percent confidence intervals with robust standard errors clustered at the country-year level. Simulations based on 10,000 draws. Observations toward the right of the panels correspond to more autocratic systems.

are not systematically attacked during election periods in more authoritarian countries.

In contrast, in the right panel, we observe a clearly positive trend when it comes to attacks on foreign hosts. The relationship between election periods and DoS attacks is stronger the more authoritarian a country is. DoS attacks on foreign hosts increase by almost 15 percent when a country that scores high on the autocracy index holds elections (compared to the country's average number of DoS attacks on foreign hosts per given year). Since most government websites host their servers within their own country, this increase suggests that during election periods in these regimes, more news and opposition websites may be targeted by DoS attacks. Furthermore, the right panel highlights that the relationship between election periods and DoS attacks becomes already positive for countries that are in the middle of the autocracy index, suggesting that already semi-democratic regimes may make use of the specificity, flexibility, and deniability of DoS attacks to attack news and opposition websites.

The Timing of DoS Attacks during Election Periods

To test Hypothesis 3, we vary the operationalization of our variable *election period*. In particular, we consider (i) the election week and two weeks before and after, (ii) the election week and one week before and after, and (iii) only the election week as bandwidths. Table 3 shows that in the foreign host models, the coefficients of the

Table 3. Relationship between Election Periods, Level of Autocracy and Denial-of-service Attacks (Country/Week).

(i) Election week (+ 2 weeks before and after)				
	Model 5	Model 6	Model 7	Model 8
	Domestic	Domestic	Foreign	Foreign
Election period	-.034* (.014)	-.033 (.034)	-.027* (.013)	-.110*** (.030)
Election period \times autocracy index		.021 (.074)		.244*** (.063)
Country \times year fixed effects	Yes	Yes	Yes	Yes
Num. obs.	81,477	70,965	28,345	24,649
(ii) Election week (+ 1 week before and after)				
	Model 9	Model 10	Model 11	Model 12
	Domestic	Domestic	Foreign	Foreign
Election period	-.020* (.014)	-.028 (.044)	-.029 (.017)	-.120** (.037)
Election period \times autocracy index		.042 (.097)		.264** (.080)
Country \times year fixed effects	Yes	Yes	Yes	Yes
Num. obs.	81,655	71,119	28,521	24,801
(iii) Only election week				
	Model 13	Model 14	Model 15	Model 16
	Domestic	Domestic	Foreign	Foreign
Election week	.020* (.014)	.001 (.072)	-.040 (.028)	-.175** (.061)
Election week \times autocracy index		.072 (.164)		.370** (.138)
Country \times year fixed effects	Yes	Yes	Yes	Yes
Num. obs.	81,840	71,280	28,704	24,960

Note: Robust standard errors clustered at the country-year level in parentheses.

*** $p < .001$.

** $p < .01$.

* $p < .05$.

interaction term increase in size the closer we move to the election week. Yet, at the same time, the level of uncertainty rises due to decreasing numbers of cases. For the domestic hosts models, the coefficients are largest when we consider the election week only. Nevertheless, the interaction term and model fit still miss conventional

Table 4. Relationship between Pre- and Postelection Periods, Level of Autocracy and Denial-of-service Attacks (Country/Week).

(iv) Preelection period				
	Model 17	Model 18	Model 19	Model 20
	Domestic	Domestic	Foreign	Foreign
Preelection period	-.037 (.019)	-.018 (.043)	-.034* (.017)	-.048 (.038)
Preelection period \times autocracy index		-.021 (.093)		.062 (.078)
Country \times year fixed effects	Yes	Yes	Yes	Yes
Num. obs.	81,283	70,795	28,153	24,481
(v) Postelection period				
	Model 21	Model 22	Model 23	Model 24
	Domestic	Domestic	Foreign	Foreign
Postelection period	-.036 (.019)	-.064 (.041)	-.019 (.016)	.136*** (.035)
Postelection period \times autocracy index		.076 (.087)		.334*** (.075)
Country \times year fixed effects	Yes	Yes	Yes	Yes
Num. obs.	81,840	71,280	28,704	24,960

Note: Robust standard errors clustered at the country-year level in parentheses.

*** $p < .001$.

** $p < .01$.

* $p < .05$.

levels of significance. Interestingly, the model highlights a small increase for the variable election week alone (model 13), suggesting a higher frequency of DoS attacks during elections weeks regardless of the regime type compared to the respective country-year average. For the foreign hosts model, the interaction effect between the election period and the autocracy index becomes stronger and remains significant the closer we move to the election week. Thus, we find support for Hypothesis 3 that expects that the increase in DoS attacks becomes stronger the closer the respective country is to an election.⁸

To further investigate whether there are differences with regard to the timing of attacks, we split the election period in a (iv) pre- and (v) postelection period (each lasting three weeks), excluding the election week as here attacks could be captured before, during, and after the election. Table 4 shows that for both dependent variables (DoS attacks against domestic and foreign hosts), the results in our main models appear to be mainly driven by DoS attacks that happen in the postelection

period and during the election week, yet, remain significant only for the foreign host models. These additional results suggest that authoritarian governments may primarily use DoS attacks in the election week and afterward to gain electoral advantages, censor accusations of electoral fraud, and/or other regime-threatening content.

Robustness Tests and Additional Models

We conduct several tests to check the robustness of our results to several coding and modeling decisions. The complete results are reported in the Online Appendix.

First, there might be the concern that the interaction models do not reflect the data generating process properly. To investigate whether this is the case, we divided the data again in democracies and nondemocratic countries using the cutoff value of 0.5. Table A.3 shows the same patterns as in our main models. The table highlights that election periods in nondemocratic regimes are on average associated with an increase by 7.91 percent (95 percent confidence intervals: 3.99 percent - 11.84 percent) of DoS attacks on foreign hosts. In contrast, for clearly democratic countries, election periods are significantly and negatively related with DoS attacks on foreign hosts. With regard to attacks on domestic hosts, the models do not find systematic relationships. Second, even though election periods are normally determined well in advance, it might be that in some cases, elections are postponed or held earlier than expected due to increasing political tension and violence in the country. In order to control for this potentially confounding factor that also may influence the frequency of DoS attacks, we add a weekly measured logged variable on the number of violent conflict events based on the Georeferenced Event Dataset for each country (Sundberg and Melander 2013). Table A.4 shows that the inclusion of this variable does not alter our results.

Third, we conduct analyses using the normalized inverted Polity 2 index of the Polity IV project (Marshall and Jaggers 2016) instead of the V-Dem index for electoral democracy. The results, reported in Table A.5, show the same patterns as compared to our main analysis. Fourth, to deal with short-term time trends, we include country-specific nonlinear time trends (cubic splines) to our models. Table A.6 shows the coefficients become smaller but remain significant for the foreign host model. Fifth, to counter concerns that our results are driven by a large number of small DoS attacks, we rerun our main models with the number of large DoS attacks as the dependent variable. We define large attacks as DoS attacks that belong to the top 30 percent of attacks on a country-year, as measured by the intensity of the data traffic used in the attack (maximal number of data packets per minute). The patterns as shown in Table A.7 are still the same.

Sixth, we run models including lagged dependent variables to our main models to address concerns about time dependencies differently (Wilkins 2018). Models A.8.1 to A.8.4 show that the directions of the coefficients remain similar when we use our main specification of election periods. Yet, the coefficient sizes become overall smaller and the coefficients display higher levels of uncertainty (but stays significant for the interaction term for the foreign host model). When we only consider the

election week, the coefficients are almost the same as in the election week model for foreign hosts reported in Table 3 (see model A.8.8), while elections alone are not anymore significantly related to an increase of domestic hosts (see model A.8.3).

Additionally, we conduct further tests addressing potential issues with our proxy for attacks on foreign hosts. First, it might be that the news websites could have changed their server location in the years from 2014 to 2017. Using historical DNS lookups from *OpenINTEL* allows us to investigate hosting patterns for a share of the news websites (those with .com, .net, and .org addresses) until 2015. While for 2016 almost 80 percent of the lookups only resolve to one unique country, this statistic decreases to 64 percent for the two years. To counter concerns of measurement errors, we run the foreign host models again for the year 2016 only, which is the year closest to our measurement. This reduces statistical power; nevertheless, the patterns of the coefficients remain the same and significant for the interaction term in the foreign host model (see Table A.9 in the Online Appendix). Second, we conduct placebo tests for our proxy for attacks on foreign hosts to counter concerns that the variable does not really capture relevant websites. To this end, we randomly assigned the proportions in which foreign countries host their news websites, excluding the foreign countries where we empirically observe the true shares. Model A.9.4 shows that we do not find a significant association anymore. Third, there might be the concern that our proxy for foreign hosts is biased as approximately 21 percent of our collected newspaper use content delivery networks, a service where regional distributed servers provide the content of websites.⁹ To investigate whether this alters our result, we recalculated our proxy for attacks on foreign hosts and run our main models again. Models A.9.5 and A.9.6 show similar results.

Finally, we investigate a potential nonlinear relationship between the level of autocracy and DoS attacks during election periods. For this, we include an additional interaction term between election periods and the autocracy index as a squared term to the regression analysis (see Table A.10). Figure 5 displays the estimated interaction effect for these models and reveals some interesting patterns. First, while the right panel (DoS attacks on foreign hosts) shows the same trend as in our main models, the positive relationship of election periods and the number of DoS attacks on foreign hosts become again smaller if the country is highly authoritarian. This may be explained by the fact that these countries also have access to other technical capabilities (e.g., national firewalls or DNS filters) to implement foreign censorship. However, as the confidence intervals are quite large for these regimes, it is likely that DoS attacks are still a frequently used tool also in highly authoritarian regimes.

Second, the left panel (DoS attacks on domestic hosts) now also displays a large positive interaction effect for election periods on domestic servers when the country is at the right end of the autocracy index, as well as small increase when it very democratic. How can we explain this? We argue that, in particular, in highly controlled regimes, opposition or critical news websites should more likely host their servers abroad to escape direct government control. Thus, increasing numbers of DoS attacks during elections on websites hosted within the country rather include

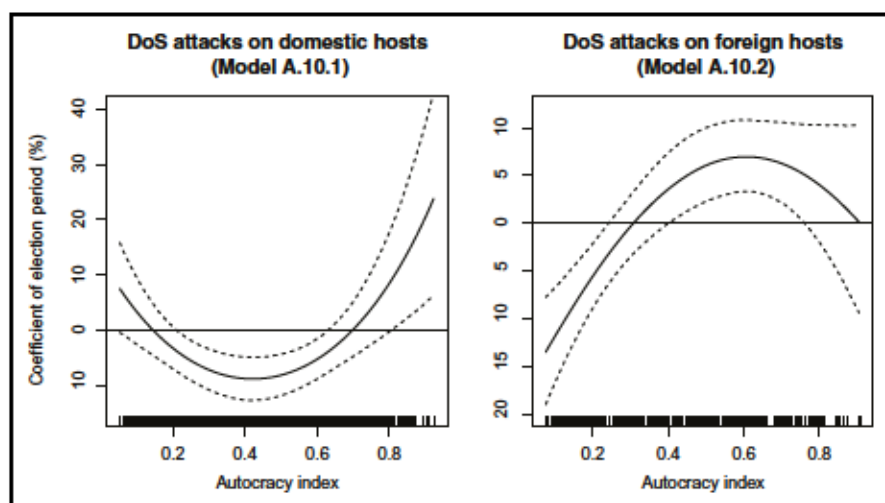


Figure 5. Interaction effect of election period dependent on the level of autocracy and its squared term; 95 percent confidence intervals with robust standard errors clustered at the country level. Simulations based on 10,000 draws. Observations toward the right of the panels correspond to more autocratic systems.

DoS attacks on government and state-related websites only. Hence, while we cannot tell for sure whether government or opposition websites were targeted domestically, it appears that the increase of DoS attacks in highly authoritarian regimes might be primarily explained by domestic and international activists targeting government(-related) websites. In these regimes, the government violates free elections in an obvious manner and uses means of increased repression. Both points foster the motivation to launch DoS attacks and make the use of DoS attacks more likely as they are less costly compared to high-risk forms of collective action, for example, street protests. With regard to the second observation (the positive relationship between election periods and DoS attacks in highly democratic countries), it may be that these attacks reflect the use of DoS attacks for interstate disputes (Valeriano and Maness 2014). Yet since this finding remains beyond conventional levels of significance, it seems that recent reports of DoS attacks by presumably Russian actors during elections in the United States, Sweden, and France appear to be (still) rather the expectation than the rule.

Conclusion

In this article, we show that DoS attacks are not only used for criminal activities but also for political purposes. While election periods in democratic countries are not related to a systematic increase in DoS attacks, we show that election periods in authoritarian countries increase the frequency of DoS attacks. In particular, our

empirical results support our theoretical expectation that authoritarian regimes are using DoS attacks to export censorship and target independent news and other opposition websites hosted abroad during periods of political contention. In these countries, we see clear evidence that the intensity of DoS attacks increases the closer the respective authoritarian regime is to an election.

Our findings have some important implications for civil society actors, NGOs, newspapers, and dissident groups in political regimes. In addition to hosting their servers abroad to escape direct government control, these actors should invest in DoS mitigation services, especially around elections and other contentious periods to protect themselves against DoS attacks. This would ensure that citizens and the global audience can still access information from independent media, even though governments or state-near groups try to disrupt their services. Future work should study methods by which these attacks could be more reliably traced back to their initiator, facilitating accountability. Researchers might also study the types of news organizations, blogs, or dissident groups that are likely to be targets of such attacks abroad.

More broadly, future research should help map how these tactics are used alongside traditional means of autocratic censorship and repression. For example, in what way do nondemocratic regimes use of DoS attacks compared to conventional means of censorship and repression? Are DoS attacks used as a complement to classical means of repression or do they partly replace them? And at what point do governments employ more drastic means of just-in-time censorship such as complete network outages?

Authors' Note

The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government. All remaining errors are our own.

Acknowledgments

We would like to thank the participants at the workshops on "Telecommunication Politics in Authoritarian Contexts" (University of St. Gallen) and "The Empirical Study of Autocracy" (University of Konstanz) for comments on earlier versions of this article. Furthermore, this article benefited greatly from presentations at the International Political Science Association (IPSA) conference on "Political Science in the Digital Age," the seventy-sixth annual Midwest Political Science Association (MPSA) conference, and the twenty-seventh German Political Science Association conference on "Frontiers of Democracy." Moreover, we would like to thank Anita Gohdes and Mark Crescenzi for helpful comments on this project. Finally, we thank the two anonymous reviewers and the editor of the *Journal of Conflict Resolution*, Paul Huth, whose comments led to major improvements of this article.

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) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Work for this project was supported by the DFG grant 402127652 and by the National Science Foundation grant CNS-1730661. This material is based on research sponsored by the Air Force Research Laboratory under agreement number FA8750-18-2-0049. This work used the Extreme Science and Engineering Discovery Environment, which is supported by the National Science Foundation grant number ACI-1053575. This work was supported by the Netherlands Organization for Scientific Research through the D3 project (628.001.018). This research made use of data from OpenINTEL, a joint project of the University of Twente, SURFnet, SIDN, and NLnet Labs.

ORCID iD

Philipp M. Lutscher  <https://orcid.org/0000-0001-6176-7297>

Nils B. Weidmann  <https://orcid.org/0000-0002-4791-4913>

Supplementary Material

Supplementary material is available online for this article.

Notes

1. Not surprisingly, most of these regimes are autocratic or illiberal democracies.
2. For a review of technical approaches to censorship, see Deibert et al. (2008).
3. An exception is a recent study by Kostyuk and Zhukov (2019) that relies on data by the private Internet company Arbor Networks. However, this approach can only capture attacks against servers equipped with Arbor's DoS mitigation technology. This technology may be used more in certain countries, which makes this measurement approach problematic for comparisons across many different countries worldwide.
4. We restricted the analysis to countries that are contained in the Correlates of War list of independent states (Singer 1988).
5. Due to the fact that the use of content delivery networks (CDNs), a service where regional distributed servers provide the content of websites, might bias the geolocation of servers, we additionally conduct robustness tests with a recalculated indicator, leaving out newspapers using this service (see Robustness Tests and Additional Models section).
6. To determine the maximal lag of the Newey–West correction, we follow a rule of thumb that sets this value to $t^{1/4}$ (Greene 2011). Respective tests for the model highlight that this correction is necessary.
7. We follow Lüthmann, Tannenbergh, and Lindberg (2018) here, who use the same threshold to distinguish between autocracy and democracy.
8. We additionally run models considering the time to closest election. We operationalize this variable as 1/time to closest election to discount weeks the further they are away from an

election. The results reported in Table A.2 highlight a positive interaction effect between temporal proximity to elections and the autocracy index for the foreign hosts model. In addition, we find a significant and positive (but clearly smaller) effect in the noninteracted foreign host model as well. In contrast, the coefficient for temporal proximity alone in the domestic hosts model is not positive anymore.

9. We retrieved information for big CDNs from Scott et al. (2016) and PAT Research (2019). These include Google, Akamai, Swarmify, Microsoft, Amazon, KeyCDN, Limelight, Cloudflare, Rackspace, CDNLion, MaxCDN, SoftLayer, Incapsula, Fastly, Dyn, Automatic, AliCloud, CDN77, Edgecast, and CacheFly.

References

- Asal, Victor, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins, and Chris Bronk. 2016. "Repression, Education, and Politically Motivated Cyberattacks." *Journal of Global Security Studies* 1 (3): 235-47.
- Beyer, Jessica L. 2014. *Expect Us: Online Communities and Political Mobilization*. Oxford, UK: Oxford University Press.
- Boas, Taylor C. 2006. "Weaving the Authoritarian Web: The Control of Internet Use in Nondemocratic Regimes." In *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology*, edited by John Zysman Abraham Newman, 361-78. Stanford, CA: Stanford University Press.
- Butler, Daren. 2011. "Turkish Websites Attacked by Anonymous Before Vote." *Reuters*, June 09. Accessed June 26, 2019. <https://www.reuters.com/article/us-turkey-election-internet/turkish-websites-attacked-by-anonymous-before-vote-idUSTRE7583DV20110609>.
- CAIDA, UC San Diego. 2016. "The CAIDA UCSD Near-real-time Network Telescope, 2008-2016." Accessed June 26, 2019. http://www.caida.org/data/passive/telescope-near-real-time_dataset.xml.
- Cardenas, Cat. 2017. "Freedom of the Press also Targeted Virtually in Venezuela, Where Cyberattacks Can Force Independent Sites Offline." Accessed June 26, 2019. <https://www.knightcenter.utexas.edu/blog/00-18194-freedom-press-also-targeted-virtually-venezuela-where-cyberattacks-can-force-independe>.
- Carr, Jeffrey. 2011. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media.
- Chen, Yuyu, and David Y. Yang. 2019. "The Impact of Media Censorship: 1984 or Brave New World?" *American Economic Review* 109 (6): 2294-332.
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso Books.
- Coppedge, Michael, John Gerring, Staffan I. Lindberg, Svend-Erik Skaaning, Jan Teorell, David Altman, Michael Bernhard, et al. 2016. "V-Dem [Country-Year/Country-Date] Dataset V6.2." Varieties of Democracy (V-Dem) Project. University of Gothenburg: Varieties of Democracy Institute.
- Dainotti, Alberto, Claudi Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russan, and Antonio Pescapé. 2014. "Analysis of Country-wide Internet

- Outages Caused by Censorship." *IEEE/ACM Transactions on Networking* 22 (6): 1964-77.
- Deibert, Ronald J., John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Gross Stein. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Boston, MA: MIT Press.
- Deibert, Ronald J., and Rafal Rohozinski. 2010. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21 (4): 43-57.
- Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. 2012. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War." *Security Dialogue* 43 (1): 3-24.
- Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21 (3): 69-83.
- Dolata, Ulrich, and Jan-Felix Schrape. 2016. "Masses, Crowds, Communities, Movements: Collective Action in the Internet Age." *Social Movement Studies* 15 (1): 1-18.
- Dragu, Tiberiu, and Yonatan Lupu. 2017. "Does Technology Undermine Authoritarian Governments?" Working Paper. New York University and George Washington University.
- Earl, Jennifer, Andrew Martin, John D. McCarthy, and Sarah A. Soule. 2004. "The Use of Newspaper Data in the Study of Collective Action." *Annual Review of Sociology* 30:65-80.
- Enikolopov, Ruben, Alexey Makarin, and Maria Petrova. 2018. "Social Media and Protest Participation: Evidence from Russia." Working Paper. Available at SSRN: <https://ssrn.com/abstract=2696236>.
- Freedom House. 2016. *Freedom of the Net 2016: Silencing the Messenger: Communication Apps Under Pressure*. Washington, DC: Freedom House.
- Freedom House. 2017. *Freedom of the Net 2017: Manipulating Social Media to Undermine Democracy*. Washington, DC: Freedom House.
- Gandhi, Jennifer, and Ellen Lust-Okar. 2009. "Elections Under Authoritarianism." *Annual Review of Political Science* 12:403-22.
- Goncharov, Max. 2012. "Russian Underground 101." *Trend Micro Incorporated*. Accessed June 27, 2019. <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>.
- Greene, William H. 2011. *Econometric Analysis, Vol. 7*. London, UK: Pearson.
- Gunitsky, Seva. 2015. "Corrupting the Cyber-commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13 (01): 42-54.
- Hardy, Seth, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill, and Ronald J Deibert. 2014. "Targeted Threat Index: Characterizing and Quantifying Politically-motivated Targeted Malware." In *Proceedings of the 23rd USENIX Conference on Security Symposium*, 527-41. San Diego: USENIX Association.
- Hassanpour, Navid. 2014. "Media Disruption and Revolutionary Unrest: Evidence from Mubarak's Quasi-experiment." *Political Communication* 31 (1): 1-24.
- Hobbs, William R., and Margaret E. Roberts. 2018. "How Sudden Censorship Can Increase Access to Information." *American Political Science Review* 112 (3): 621-36.

- Holt, Thomas J., Max Kilger, Lichun Chiang, and Chu-Sing Yang. 2017. "Exploring the Correlates of Individual Willingness to Engage in Ideologically Motivated Cyberattacks." *Deviant Behavior* 38 (3): 356-73.
- IFES ElectionGuide. 2017. "ElectionGuide: Democracy Assistance & Election News." Accessed June 27, 2019. <https://www.electionguide.org>.
- Internet Society. 2015. "Addressing the Challenge of IP Spoofing." Technical Report. Accessed June 27, 2019. <https://www.internetsociety.org/doc/addressing-challenge-ip-spoofing>.
- Jagannathan, Malavika. 2012. "DDoS Attacks Disable Independent News Sites During Russian Protests." *Herdict Blog*, June 14. Accessed June 27, 2019. <https://blogs.harvard.edu/herdict/2012/06/14/ddos-attacks-disable-independent-news-sites-during-russian-protests/>.
- Jonker, Mattijs, Alistair King, Johannes Krupp, Christian Rossow, Anna Sperotto, and Alberto Dainotti. 2017. "Millions of Targets under Attack: A Macroscopic Characterization of the DoS Ecosystem." In *Proceedings of the 2017 Internet Measurement Conference*, 100-13. London: ACM.
- Jordan, Tim. 2002. *Activism! Direct Action, Hacktivism and the Future of Society*. London, UK: Reaktion Books.
- Karnej, Ihar, and Brian Whitmore. 2008. "Belarus: RFE/RL Cites Online 'Solidarity' in Face of Cyberattack." *Radio Free Europe*, April 29. Accessed June 27, 2019. <https://www.rferl.org/a/1109649.html>.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107 (2): 1-18.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review* 111 (3): 484-501.
- Knutsen, Carl Henrik, Håvard Moksleiv Nygård, and Tore Wig. 2017. "Autocratic Elections: Stabilizing Tool or Force for Change?" *World Politics* 69 (1): 98-143.
- Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63 (2): 317-47.
- Lindberg, Steffan I. 2009. *Democratization by Election: A New Mode of Transition*. Baltimore, MD: Johns Hopkins University Press.
- Little, Andrew T. 2012. "Elections, Fraud, and Election Monitoring in the Shadow of Revolution." *Quarterly Journal of Political Science* 7 (3): 249-83.
- Little, Andrew T. 2016. "Communication Technology and Protest." *The Journal of Politics* 78 (1): 152-66.
- Lührmann, Anna, Marcus Tannenberg, and Staffan I. Lindberg. 2018. "Regimes of the World (RoW): Opening New Avenues for the Comparative Study of Political Regimes." *Politics & Governance* 6 (1): 60-77.
- MacKinnon, Rebecca. 2013. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.
- Magaloni, Beatriz. 2008. "Credible Power-sharing and the Longevity of Authoritarian Rule." *Comparative Political Studies* 41 (4-5): 715-41.

- Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, et al. 2015. "An Analysis of China's 'Great Cannon'." In *Proceedings of the 5th USENIX FOCI Workshop*. Washington, DC: USENIX Association.
- Marshall, Monty G., and Keith Jagers. 2016. *Polity IV Project: Political Regime Characteristics and Transitions, 1800-2016*. Vienna, VA: Center for Systemic Peace.
- Milan, Stefania. 2015. "Hacktivism as a Radical Media Practice." In *The Routledge Companion to Alternative and Community Media*, edited by Chris Atton, 550-60. London, UK: Routledge.
- Moore, David, Colleen Shannon, Douglas J. Brown, Geoffrey M. Voelker, and Stefan Savage. 2006. "Inferring Internet Denial-of-Service Activity." *ACM Transactions on Computer Systems (TOCS)* 24 (2): 115-39.
- Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.
- Nazario, Jose. 2009. "Politically Motivated Denial of Service Attacks." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck Kenneth Geers, 163-81. Washington, DC: IOS Press.
- Olson, Parmy. 2013. *We Are Anonymous*. New York: Random House.
- Olson, Parmy. 2014. "The Largest Cyber Attack in History Has Been Hitting Hong Kong Sites." *Forbes Magazine*, November 20. Accessed June 27, 2019. <https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/>.
- PAT Research. 2019. "Top 16 Content Delivery Network Providers." Accessed June 27, 2019. <https://www.predictiveanalyticstoday.com/top-content-delivery-network-providers/>.
- Pearce, Katy E., and Sarah Kendzior. 2012. "Networked Authoritarianism and Social Media in Azerbaijan." *Journal of Communication* 62 (2): 283-98.
- Qurium, The Media Foundation. 2017. "News Media Websites Attacked from Governmental Infrastructure in Azerbaijan." March 10. Accessed June 27, 2019. <https://www.qurium.org/news-media-websites-attacked-from-governmental-infrastructure-in-azerbaijan/>.
- Roberts, Hal, and Bruce Etling. 2011. "Coordinated DDoS Attack During Russian Duma Elections." *Internet & Democracy Blog*, December 08. Accessed June 27, 2019. <http://blogs.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/>.
- Roberts, Margaret E. 2018. *Censored: Distraction and Diversion Inside Chinas Great Firewall*. Princeton, NJ: Princeton University Press.
- Sauter, Molly. 2014. *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Publishing.
- Schedler, Andreas. 2013. *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford, UK: Oxford University Press.
- Scott, Will, Thomas Anderson, Tadayoshi Kohno, and Arvind Krishnamurthy. 2016. "Satellite: Joint Analysis of CDNs and Network-level Interference." In *2016 USENIX Annual Technical Conference (ATC)*, Denver: USENIX Association.

- Shirah, Ryan. 2016. "Electoral Authoritarianism and Political Unrest." *International Political Science Review* 37 (4): 470-84.
- Singer, J. David. 1988. "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816-1985." *International Interactions* 14 (2): 115-32.
- Sundberg, Ralph, and Erik Melander. 2013. "Introducing the UCDP Georeferenced Event Dataset." *Journal of Peace Research* 50 (4): 523-32.
- The Australian. 2011. "Malaysian News Site Attacked." *The Australian*, April 14.
- The Turkish Newswire. 2014. "Most Companies Vulnerable to Cyber Threat, Report Says." *The Turkish Newswire*, April 04.
- Tucker, Joshua A. 2007. "Enough! Electoral Fraud, Collective Action Problems, and Post-communist Colored Revolutions." *Perspectives on Politics* 5 (03): 535-51.
- Tucker, Joshua A., Yannis Theochanis, Margaret E. Roberts, and Pablo Barberá. 2017. "From Liberation to Turmoil: Social Media and Democracy." *Journal of Democracy* 28 (4): 46-59.
- Valeriano, Brandon, and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11." *Journal of Peace Research* 51 (3): 347-60.
- Van Laer, Jeroen, and Peter Van Aelst. 2010. "Internet and Social Movement Action Repertoires: Opportunities and Limitations." *Information, Communication & Society* 13 (8): 1146-71.
- van Rijswijk-Deij, Roland, Mattijs Jonker, Anna Sperotto, and Aiko Pras. 2016. "A High-performance, Scalable Infrastructure for Large-scale Active DNS Measurements." *IEEE Journal on Selected Areas in Communications* 34 (6): 1877-88.
- Villeneuve, Nart, and Masashi Crete-Nishihata. 2012. "Control and Resistance: Attacks on Burmese Opposition Media." In *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, edited by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 153-76. Boston, MA: MIT Press.
- Weidmann, Nils B., Doreen Kuse, and Kristian Skrede Gleditsch. 2010. "The Geography of the International System: The CShapes Dataset." *International Interactions* 36 (1): 86-106.
- Wilkins, Arjun S. 2018. "To Lag or Not to Lag?: Re-evaluating the Use of Lagged Dependent Variables in Regression Analysis." *Political Science Research and Methods* 6 (2): 393-411.
- Wong, Wendy H., and Peter A. Brown. 2013. "E-bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One." *Perspectives on Politics* 11 (04): 1015-33.
- Yildirim, A. Kadir. 2016. *Muslim Democratic Parties in the Middle East: Economy and Politics of Islamist Moderation*. Bloomington: Indiana University Press.
- Zargar, Saman Taghavi, James Joshi, and David Tipper. 2013. "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks." *IEEE Communications Surveys & Tutorials* 15 (4): 2046-69.
- Zuckerman, Ethan, Hal Roberts, Ryan McGrady, Jillian York, and John Palfrey. 2010. *Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites*. Cambridge, MA: The Berkman Center for Internet & Society, Harvard University.