Political Science Research and Methods (2023), **11**, 696–711
doi:10.1017/psrm.2021.68

ORIGINAL ARTICLE

Hot topics: Denial-of-Service attacks on news websites in autocracies

Philipp M. Lutscher

Department of Political Science, University of Oslo, Oslo, Norway
Corresponding author. Email: philipp.lutscher@stv.uio.no

(Received 11 November 2020; revised 8 June 2021; accepted 29 August 2021; first published online 6 December 2021)

Abstract

Most authoritarian countries censor the press. As a response, many opposition and independent news outlets have found refuge on the Internet. Despite the global character of the Internet, news outlets are vulnerable to censorship in cyberspace. This study investigates Denial-of-Service (DoS) attacks on news websites in Venezuela and details how news reporting is related to DoS attacks in an attempt to censor content. For this empirical test, I monitored 19 Venezuelan news websites from November 2017 until June 2018 and continuously retrieved their content and status codes to infer DoS attacks. Statistical analyses show that news content correlates to DoS attacks. In the Venezuelan context, these news topics appear to be not only on protest and repression but also on opposition actors or other topics that question the legitimacy of the regime. By establishing these relationships, this study deepens our understanding of how modern technologies are used as censorship tools.

Keywords: autocratic politics; censorship; cyberattacks; text and content analysis; data collection

1. Introduction

Most authoritarian governments censor the press (Stier, 2015). In the past, it was quite difficult for media outlets to evade press censorship. Today, with the help of the Internet, this appears to be more feasible. The Internet can provide news outlets with a way to circumvent censorship and still reach domestic and global audiences. Yet, even in this global network outlets are vulnerable to censorship and repression. While previous studies describe how governments use legal and technical means to censor online (e.g., Deibert *et al.*, 2008), the use of cyberattacks for this purpose has received relatively little academic attention.

Studies suggest that one type of cyberattack, so-called Denial-of-Service (DoS) attacks, frequently target news and other websites during contentious times in authoritarian regimes (Nazario, 2009; Global Voices, 2011; Cardenas, 2017; Lutscher *et al.*, 2020). These attacks flood servers with high levels of Internet traffic, making them temporarily inaccessible for Internet users worldwide. For instance, when self-declared Venezuelan president, Juan Guaidó, returned to Caracas in March 2019 to continue his political fight against the Maduro government, several newspapers were hit by DoS attacks at the same day (Rosas, 2019). Beyond Venezuela, reports on DoS attacks against Russian newspapers when they reported on electoral fraud in December 2011 (Global Voices, 2011), Burmese outlets during contentious periods (Nazario, 2009), or attacks on Turkish newspapers (The Turkish Newswire, 2014) show similar patterns.

Nevertheless, systematic evidence on when, why, and what online newspapers are targeted in autocracies remains scarce. In this paper, I explore whether reporting on specific news topics increases the likelihood of DoS attacks on news websites. Where the introductory examples, and many more that follow below, provide anecdotal evidence that critical reporting may lead to DoS attacks, I continuously monitored the status and reporting of several private and independent Venezuelan news websites from November 2017 until June 2018 to explore this relationship systematically. With this approach, I address two important problems in the study of cyber attacks. First, I avoid selection bias since I do not only look at the attacked website and its published content on the day of attack. Second, I avoid reporting biases because DoS attacks against independent outlets are often unreported (Hardy *et al.*, 2014; Maschmeyer *et al.*, 2020).

Since it is *a priori* unknown what news outlets report on, I used topic models to create 50 topics reported on by Venezuelan newspapers and sorted them into broader categories expected to be censor-worthy in the Venezuelan context: news about protests and repression, socio-economic mismanagement, and pieces that question the political legitimacy of the regime such as electoral issues and news about opposition actors. Following this, I ran statistical models controlling for newspapers and time-related factors to investigate what topics are related to a higher likelihood of DoS attacks. The main and additional models show that several of the hypothesized censor-worthy topics correlate positively to the likelihood of being targeted by a DoS attack. Most topics either seem to question the political legitimacy of the regime or report on protests and repression.

The Venezuelan case is not only relevant to study as there have been incidents of DoS attacks linked to the Maduro government (La Patilla, 2018*b*; Galicia Lugo, 2019), but also because the regime has become more authoritarian in recent years. Due to increasing levels of press censorship, online outlets remain often the only independent information source for citizens in Venezuela (Cardenas, 2017; OONI, 2018). While previous studies explored sophisticated online censorship strategies primarily in China (e.g., Roberts, 2018), research on other countries as well as technologically simpler censoring tools are still rare. Moreover, by showing that it is not only protest-related topics that are associated with an increased likelihood of DoS attacks in Venezuela, this paper contributes to the growing literature on authoritarian information control (e.g., King *et al.*, 2013; Munger *et al.*, 2018; Roberts, 2018). In electoral autocracies it seems that not only protest and repression events are censor-worthy, but also reports on opposition actors and other topics that may threaten the regime's political legitimacy.

2. DoS attacks to increase information friction

2.1 Why launch DoS attacks?

Previous literature on information control in the digital age describes how governments censor online (Deibert *et al.*, 2008), finds macro-level evidence that countries censor political and news websites (Pearce *et al.*, 2017), and shows that domestic and regional unrest increase online censorship efforts in autocracies (Hellmeier, 2016). King *et al.* (2013) found that social media posts in China are deleted when they contain collective action potential, while recent studies suggest that posts that are critical of the government may also be censored (Gueorguiev and Malesky, 2019). Other research has emphasized that modern-day authoritarian governments do not only rely on deletion to control information, but use the Internet and social media to distract from sensitive content (King *et al.*, 2017; Spaiser *et al.*, 2017; Munger *et al.*, 2018) or to identify and harass opposition actors (Pan and Siegel, 2020; Xu, 2020; Pearce and Kendzior, 2012).

Roberts (2018) combines these different insights on information control and proposes that censorship works through three non-exclusive mechanisms: fear, flooding, and friction. Fear can deter media institutions from distributing, and individuals from consuming, certain content. For instance, governments can pass censorship laws that forbid individuals or media institutions to write about particular topics; opposition activists are often intimidated and media outlets publicly sanctioned for reporting on specific subject matter. Flooding, in contrast, increases the relative costs to consumers who wish to retrieve information and can be achieved by distributing pro-regime messages and/or literally flooding social media channels with content. Finally, friction increases the costs to individuals and organizations seeking to gain access to and distribute sensitive information—often covertly—blocking specific websites or restricting access to information in other ways. Whereas the permanent censorship of specific websites is a good example of this mechanism, even a slightly slower loading website increases friction costs.

Previous qualitative and quantitative evidence suggests that DoS attacks frequently target news websites in autocracies in an attempt to disrupt information flows (Deibert *et al.*, 2008; Global Voices, 2011; Freedom House, 2016; Lutscher *et al.*, 2020; Nazario, 2009). Compared to more sophisticated (e.g., firewalls or filters) or brute-force (e.g., network shutdowns) forms of online censorship, DoS attacks have some useful properties as a censoring tool. First, DoS attacks can target websites worldwide, enabling governments to temporarily disable sites in cases where authoritarian administrations cannot employ pressure on providers to block them. Second, DoS attacks often go unnoticed and are hard to trace back. Users are unaware that a particular website has been hit by a DoS attack and even if such attacks should become public, governments will often deny any involvement (Lutscher *et al.*, 2020).

In this paper, I argue that the main mechanism through which politically-motivated DoS attacks on news websites work is through information friction: they increase the costs for individuals and outlets to gain access to and distribute information. Table 1 summarizes how DoS attacks can increase friction costs distinguishing between news consumers versus providers and between temporary versus long-term costs.

(a) If successful, the temporary cost of a DoS attack for consumers is that a complete news website is unavailable for a specific, potentially critical, point in time. DoS attacks make it harder and more costly for domestic citizens and the global audience to access information. The average Internet user will see only that the website is not accessible or is loading very slowly and will not spend extra effort to search for the reasons for the outage. Several studies show that when it comes to information consumption in the digital age, the average consumer is extremely impatient and will opt to visit other websites if they have to wait longer than usual (Brutlag, 2009; Athey and Mobius, 2012). Evidently, politically engaged individuals may be less impatient and notice that the website has been purposely taken offline. As stated by Roberts (2018), the goal of information friction is, however, not to completely restrict access to information but rather increase the average costs involved in retrieving undesirable content.

(b) Beyond temporary costs, DoS attacks may also increase fees borne by consumers to access specific information in the long-term. When Internet users observe frequent outages or high latencies in a website, they are likely to switch permanently to other more stable websites due to the simple reason that it requires too much patience to access the specific site (see above). Beyond these increased costs to website access, it may also be that readers find the website to no longer be reliable and credible because it is frequently offline (cf. Klyueva, 2016).

(c) For news outlets, DoS attacks likewise increase costs in the short-term if they still want to provide content. News providers are forced to employ IT experts, hire DoS mitigation services, or look for alternative ways to provide information. Moreover, money is lost if they are unreachable because no users see their advertising, which constitutes the primary income for news websites (Mitchelstein and Boczkowski, 2009).

(d) A long-term consequence of, in particular, frequent DoS attacks may be that outlets will alter their content. News websites may do so to avoid future DoS attacks that accumulate the temporary costs outlined in (c). Moreover, outlets may potentially decide to self-censor because fewer users are visiting due to the long-term cost to the consumer described in (b). Finally, DoS attacks may also be understood as a signal to outlets that

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

Table 1. DoS attacks and friction costs

	Temporary costs	Long-term costs
Consumer	(a) No access to information	(b) Unreliable information
Provider	(c) No provision of information/economic costs	(d) Self-censoring of information

more drastic means such as permanent censorship will follow if they do not alter their content. Obviously, this potential consequence of DoS attack works only if editors or website owners are aware that such attacks are somehow related to their published content, and when attacks can generate enough pressure on the outlet.

2.2 When to launch DoS attacks?

When authoritarian regimes are indeed relying on DoS attacks to increase friction costs, the question remains—when should we expect the use of these attacks? Given that DoS attacks are quick and easy to employ in addition to being rather inexpensive, it could be expected that critical news websites are constantly hit. As previously noted, however, steps can be taken to protect news websites by switching the IP address or hiring DoS mitigation services, making it more difficult and expensive to constantly attack. More importantly, the advantage of DoS attacks as a concealed friction tool likely diminishes instances when they are launched for a longer period. The public may discover that there is a reason for the outage and potentially gain more interest in the attacked site (cf. Martin, 2007). If the perpetrators use these attacks to increase friction costs, it is likely that they are launched against news outlets as a response to the reporting of specific news. In particular, if the main goal of DoS attacks is to temporarily censor, regimes are likely to use DoS attacks relatively soon after news outlets have published undesirable information. But what topics are deemed censor-worthy by authoritarian regimes?

First, one main threat to the survival of an autocrat remains popular contention (Svolik, 2012). Theoretical models expect the use of censorship and other means of information control during contentious periods (Edmond, 2013; Gehlbach and Sonin, 2014). Empirical studies from China show that social media posts reporting on protests or events that have direct collective action potential, e.g., repressive events, are likely to be censored (King *et al.*, 2013). Beyond China, already Rasler (1996) detailed how the Shah regime used means of press censorship in a response to mass protests during the Iranian revolution in 1979. Concerning the use of DoS attacks, anecdotal evidence suggests that authoritarian regimes employ these in a similar fashion. For instance, in May 2012, Russian newspapers were targeted when they reported about a large-scale protest against the inauguration of President Putin (Jagannathan, 2012). In 2016, Ecuadorian news websites suffered DoS attacks when they reported on protest events (Freedom House, 2016).

Second, recent work on autocratic politics contends that the main legitimacy strategy of modern-day autocracies centers around economic performance (Guriev and Treisman, 2019). In fact, economic downturns may also spur citizens to engage in opposition activities as they open a window of opportunity and increase grievances (Dorsch *et al.*, 2015). While Rozenas and Stukal (2019) do not find that Russian state media is actively censoring bad news on the economy but instead shifts the blame to external actors, it may still be that opposition or independent outlets encounter censorship when reporting about social and economic grievances. In particular, the potential long-term costs of DoS attacks may be helpful in this regard as users could become less likely to visit targeted websites and news outlets may even alter the content to avoid such an outcome. In the Venezuelan case, there is indeed evidence that the regime wishes to censor such information. For example, state-owned Venezuelan Internet service providers have attempted to block the outlet *DolarToday* since 2014. This website writes predominantly about the country's worsening economic condition (Rueda, 2015).

Third, news that questions the overall political legitimacy of a regime may be deemed censorworthy. In the context of an electoral autocracy, this especially includes reports on opposition actors and electoral malpractices. As noted by Tucker (2007), accusations of electoral fraud may serve as a focal point for political protest and are thus perceived as threatening by the regime. Furthermore, reports on the opposition in electoral autocracies may further make citizens aware of a credible alternative and reduce the political support for the authoritarian government. More generally, however, it can be various topics that question the political legitimacy of an authoritarian regime. To name just a few, authoritarian regimes may want to avoid reports on corruption accusations, resignation demands, or other governments or simply the outlet itself questioning the regime's political legitimacy. Publicly questioning the regime's legitimacy could again ultimately increase the likelihood of contention against the regime (cf. Walker *et al.*, 1988).

Concerning the use of DoS attacks, there is indeed widespread evidence that news outlets were hit by DoS attacks when they have reported on such topics. The Russian website *Vedomist* was attacked following a series of articles that were critical of the authorities (BBC, 2009). *El Pitazo*, a Venezuelan news website, suffered from DoS attacks in March 2017 after publishing several articles about vice-president Tareck El Aissami links to drug-trafficking (Cardenas, 2017). Similarly, DoS attacks occurred against Belorussian media outlets after stories were run about students being forced to attend a public pro-government prayer in 2015 (Freedom House, 2016). Related to electoral and opposition topics, outlets in Russia were hit by large-scale and prolonged DoS attacks before the 2011 Durma election when an electoral fraud map was published (Global Voices, 2011), and several Venezuelan news websites were attacked in 2019 when they reported on the return of Venezuelan's self-declared interim president, Juan Guaidó, to Caracas (Rosas, 2019).

To summarize, I expect the following:

Hypothesis 1: Reporting on protests or repression increases the likelihood of DoS attacks against news outlets in autocracies.

Hypothesis 2: Reporting on socioeconomic mismanagement increases the likelihood of DoS attacks against news outlets in autocracies.

Hypothesis 3: Reporting on regime-delegitimizing topics increases the likelihood of DoS attacks against news outlets in autocracies.

Finally, I expect that more widespread coverage of a topic will lead to a greater likelihood of DoS attacks since the topic is more salient and encountered by more readers.

3. Research design

To explore my theoretical expectations, I focus on Venezuela and monitor several Venezuelan news websites. The next subsection introduces the Venezuelan case, which is followed by a description of the sample and an explanation about how DoS attacks were measured for this study. I subsequently describe the text data and the topic model approach used. Lastly, I describe the statistical method and empirical strategy.

3.1 The case of Venezuela

In the second half of the 20th century, Venezuela was one of the few democratic countries in South America. During the incumbency of Hugo Chávez which began in 1999, the country began to follow an authoritarian path. After the death of Hugo Chávez in 2013, the former vice-president Nicolás Maduro took over power. Since then, the country has faced an escalating

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

socioeconomic crisis (Munger *et al.*, 2018). In December 2015, the incumbent government lost its majority in the *Asamblea Nacional de Venezuela*. The government response was with harsh repression, the creation of the pro-government filled Constituent National Assembly, and increasing levels of press censorship. Concerning the latter, the regime has managed to almost gain entire control over traditional media, making it hard to retrieve critical views from print and broadcast media (Hawkins, 2016; Freedom House, 2017*a*).

As a response, most media outlets have migrated to the Internet, making news websites of particular importance for Venezuelan citizens to retrieve independent news (Cardenas, 2017). The regime has reacted to this by setting up pro-government websites, uses social media as a distraction (Munger *et al.*, 2018), and has its own pro-government online agitators (Morales, 2019). Moreover, government-owned Internet Service Providers (ISPs) have begun to filter some websites in recent years and news and other websites are increasingly hit with DoS and other technical attacks (Freedom House, 2017*b*; OONI, 2018; La Patilla, 2018*b*; Franceschi-Bicchierai, 2019). Official documents indeed confirm that the Venezuelan armed forces have dedicated cyber units and investigative reports link DoS attacks against Venezuelan news outlets back to these units (Galicia Lugo, 2019).

Apart from the frequent use of DoS attacks in Venezuela and the important focus on news outlets as information gatekeepers, the case of Venezuela enhances our knowledge as to how modern technologies are employed as a censoring tool in electoral autocracies beyond the well-studied case of China (King *et al.*, 2013; Roberts, 2018). More precisely, this study focuses on the period from November 2017 to June 2018, which includes the municipal elections held on 10 December 2017, and the presidential election on 20 May 2018. This period was chosen as previous studies have reported an increase in DoS attacks during election periods (Lutscher *et al.*, 2020).

Although Nicolás Maduro was able to win the presidential election with almost 70 percent of the votes, the election was characterized by a ban on opposition candidates, a boycott by most of the opposition, the lowest turnout in Venezuelan history, and (plausible) accusations of electoral fraud (Sen, 2018). More precisely, *Mesa de la Unidad Democrática* (MUD), the largest opposition alliance decided to boycott the election after the national election council, the *Consejo Nacional Electoral* (CNE), disqualified the most threatening opposition candidates. These candidates included Henrique Capriles, who almost won the 2013 presidential election, and Leopold Lopez and Antonio Ledezma, who are former political prisoners and popular conservative opposition actors (Herrero and Semple, 2018).

3.2 Sample and measurement of DoS attacks

Previous studies emphasize that DoS attacks on civil society and news websites in autocracies are often underreported (Hardy *et al.*, 2014; Maschmeyer *et al.*, 2020). To improve upon previous work, my approach aims to actively measure DoS attacks on news websites.

The list of websites comes from www.abyznewslinks.com, a website that collates news outlets worldwide. I restricted the sample to websites that are not clearly associated with the state as the goal of this paper is to explore the use of DoS attacks as a censorship tool against private, independent, or opposition outlets. I added this restriction as activists may also use DoS attacks against government websites (Lutscher *et al.*, 2020).[1] I did not consider inactive news websites (with no updated content), those from which content could not be downloaded, sites that purely aggregate news from other websites, or English language websites. As described in Appendix A in more detail, this left 19 websites.

Next, I set up a server with a university IP address outside Venezuela that monitored the online status of the news website sample every 30 minutes. I relied on an external server as

[1] Figure A.1 in Online Appendix A shows that my measurement also captured two potential attacks against government-affiliated websites.

DoS attacks restrict worldwide access to the targeted website, not only within the country. Moreover, by using a university server and running the measurement every 30 minute, I aimed (1) to avoid being classified as a bot, which would lead to the constant blocking of my machine, and (2) to save the computational resources on the news websites. While a greater description of the measurement approach is provided in Online Appendix A, I exploited the fact that web devices communicate according to standardized protocols. When a contacted server responds with a "503" code this indicates that the server is temporarily unavailable, most likely caused by an overload in traffic. While this is the main observable consequence of a successful DoS attack, there may also be other reasons for server overload, most prominently, maintenance work or just random errors due to the server configurations being used or legitimate latency testing, etc.[2]

To minimize the number of false positives, I impose two restrictions on my measurement. First, I do not consider measurements for the period from 12.00 to 6 a.m., when major service providers schedule maintenance work (Richter *et al.*, 2018). Second, I only consider a website as having been attacked if two subsequent measurements return a 503-error code. Although I may miss potential attacks by enforcing the second restriction, previous research shows that DoS attacks last on average between 18 and 48 minute (Jonker *et al.*, 2017). In later sensitivity tests, I relax on this restriction.

Somehow complicating the measurement task, a domain lookup shows that many of the websites in my sample are protected by Cloudflare—a popular DoS mitigation service. Protection by DoS mitigation services does not necessarily mean that such attacks cannot be successful, they still can when they extend the "protected" bandwidth or exploit other server weaknesses. Moreover, Cloudflare-protected servers also return a 503-error code when the server is placed in "under attack" mode, enabling me to also capture attack attempts for these cases (Cloudflare, 2020).[3]

Nevertheless, it is still possible that my measurement suffers from measurement error and that I wrongly infer from a 503-error code that the server is under attack. However, as long as these errors occur randomly, they "only" worsen the precision of the later statistical analysis, but not its inference. When these errors correlate systematically to news content this could lead to biases. The latter may occur when specific news attracts a large readership, causing a server overload. To control for this scenario, I include a variable measuring legitimate traffic in later robustness tests.

Figure 1 details the status of the 19 newspapers for the period from 13 November 2017, until 3 June 2018. The figure highlights that six websites likely suffered from DoS attacks at least once and that there were in total 19 attack days. The most frequently affected website is *Aporrea*, which is a leftist opposition outlet that had been loyal to the Chávez regime and which has a known history of DoS attacks (IPYS, 2017). Others that were attacked were critical opposition outlets *La Patilla* and *El Nacional*, as well as the private news websites *Confirmando*, *Informe21* and *Noticierodigital*. In fact, after the period of study, the Maduro government began to (temporarily) censor *La Patilla* and *El Nacional* at the ISP level (La Patilla, 2018*a*). More recently, state-owened ISPs also placed *Aporrea* on a block list (Aporrea, 2021). Finally, the figure shows that attacks against multiple websites seem to cluster around the municipal and presidential elections.

In sum, the descriptive results suggest that DoS attacks are a rather rare phenomenon but that they more frequently target critical news websites and that political events increase the likelihood

[2] Although, it is more likely that servers return the broader 500 error code when they encounter unspecific errors.

[3] While websites could constantly enable this mode, Figure 1 shows that for no website is this the case. Furthermore, whereas websites may return a 503 code as a response to automated requests, it would be reasonable to expect such blocking to occur for the whole period and the same service providers since my IP address and request patterns did not change. Besides, I consider the Cloudflare-specific error code "524" to be a DoS attack that is returned when Cloudflare cannot connect to the original server because the server is likely suffering from traffic overload.

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

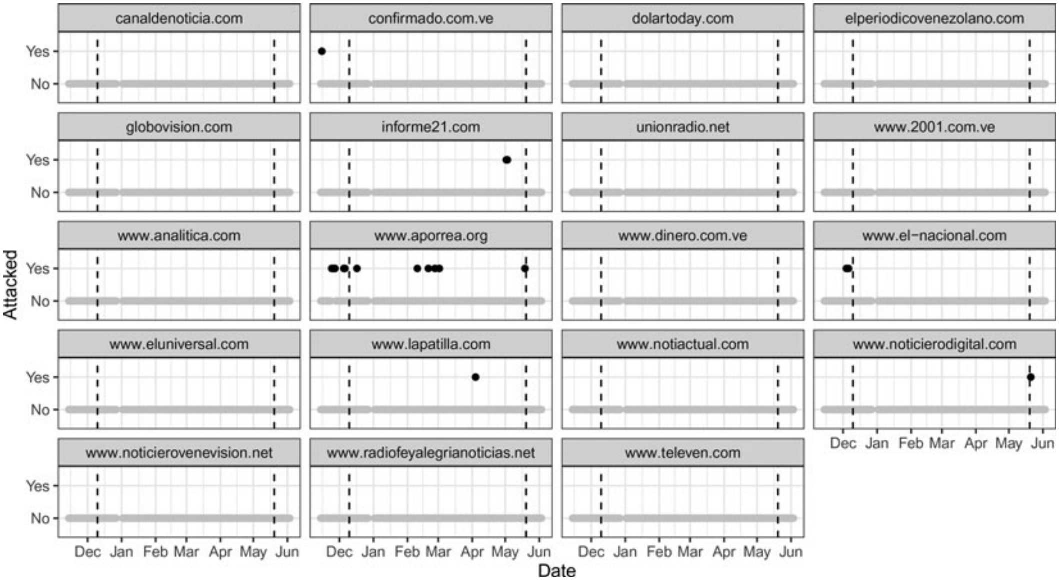

Fig. 1. Incidents of measured DoS attacks in Venezuela November 2017–June 2018. *Note*: The two vertical lines show the municipal election (10 December 2017) and presidential election (20 May 2018). Blank periods indicate time periods where the measurement did not work.

of DoS attacks (cf. Lutscher *et al.*, 2020). Concerning the attack duration, Figure A.2 in Online Appendix A illustrates that many attacks lead to short outages, while the maximum is sixteen 503-errors per day.

3.3 News retrieval and topic modeling

To retrieve the content from the websites, I downloaded the first page every day at 01:00 p.m. Venezuelan time. Next, the extraction of headlines was custom-tailored, including the first paragraph if available. In this process, uninformative headlines with less than three words were ignored along with websites structured according to broader categories, providing entertainment news, sport, culture, and technology. Finally, the headlines were parsed following standard text preprocessing procedures. Infrequent terms were not, however, removed as the content that might trigger DoS attacks could be rare. Online Appendix E presents a more detailed discussion of these steps.

To investigate whether specific news topics are related to DoS attacks, I first reduce the high dimensionality of the textual data, using topic model approaches to link the headlines to broader topics. Since Latent Dirichlet Allocation (LDA) models perform poorly with short texts, I employ the so-called Biterm Topic Model (BTM) that learns topics by modeling word-word co-occurrences patterns in the whole corpus (Yan *et al.*, 2013). For example, when the words economy, recession, and crisis frequently co-occur in headlines, irrespective of where and in what order, the algorithm identifies these terms as belonging to the same topic.

As with other unsupervised topic models, it is necessary to specify the number of topics (K) in advance. $K = 50$ was set as a good trade-off between the level of aggregation and specificity for each topic. As shown in Online Appendix E, sensitivity tests with $K = 25$ and $K = 100$ emphasize that the former identifies too many mixed topics and with the latter, it becomes difficult to differentiate between topics. For the algorithm to run, the conjugate priors α and β must be defined. I followed the specification in Yan *et al.* (2013) for short text by setting $\alpha = 50/K$ and $\beta = 0.01$. The algorithm ran using Gibbs sampling with 2000 iterations.

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

Table 2. Top 10 identified topics

P(z)	Label	Top 15 words
0.066	General opinion	Venezuela, country, continue, can, Venezuelan, politics, will be, should, alone, economy, live, make, social, Maduro, could
0.044	Sanctions	Venezuela, USA, sanction, United, government, embassy, Venezuelan, Maduro, country, European, Union, EU, election, reject, officials
0.041	National assembly	National, assembly, dispute, president, AN, politics, Venezuela, constituent, Maduro, government, commission, party, ensure, new, ANC
0.040	Maduro	Maduro, president, Nicolas, Venezuela, government, Venezuelan, ensure, announce, national, republic, election, country, new, presidential, Santos
0.039	Opposition candidate	Falcon, candidate, presidential, Henri, election, Maduro, opposition, vote, candidacy, party, president, electoral, Venezuelan, ensure, government
0.038	Government-opposition dialog	Dialog, government, opposition, Venezuelan, Dominican, Venezuela, Republic, agreement, president, Jorge, meeting, chancellor, Maduro, Rodriguez, national
0.036	Election	Election, electoral, presidential, CNE, national, council, elections, party, vote, process, president, next, municipal, realize, Venezuela
0.034	Migration crisis	Venezuelan, country, Venezuela, Colombia, crisis, international, Brazil, humanitarian, border, migration, help, thousands, refugees, national, citizens
0.031	Protest/shortages	Protest, San, missing, municipal, city, sector, neighbor, national, new, bolivar, denounce, street, transport, regional, habitat
0.031	Óscar Pérez/repression	Perez, Oscar, assassinate, body, official, steal, police, men, two, kill, CICPC, national, dead, year, Venezuelan

Note: Words are translated and unstemmed. *P*(*z*) shows the distribution of the topics over the whole corpus. The word order reflects the importance of the words.

Next, each topic was labeled by interpreting the top 15 terms per topic.[4] Table 2 shows the Top 10 topics. These topics reflect widely discussed news in 2017 and 2018: sanctions, elections, migration, and the killing of Óscar Pérez, a former elite soldier who aimed to overthrow the government. The fact that the term Venezuela often appears is that the monitored news websites report on worldwide news but unsurprisingly mostly about issues within Venezuela.

To investigate the validity of the topics, I examined their semantic validity, checking whether the generated topics are coherent and overlap with the respective headlines, as well as predictive validity by investigating whether the assigned headlines reflect real-world developments (Grimmer and Stewart, 2013). Both evaluations confirm that the model performs quite well in finding valid topics (see Online Appendix E for details).

3.4 Method

To analyze the data, the DoS measurement and topic model data were merged on the newspaper/day level. To ensure that the potential attack happened after I had downloaded the content, I define a day as lasting from 1 p.m. until 1 p.m. the next day. Since it is expected that topics with broader coverage will increase the incentive to use DoS attacks the most, I aggregated the generated topics to their mean value for a given newspaper/day.

Next, I used a penalized logistic regression with a Firth bias correction as my estimator (Firth, 1993). This commonly-used bias correction can produce finite parameter estimates even in the case of quasi- or complete separation, an issue that commonly occurs with rare events. Cook *et al.* (2020) show that this correction for the inclusion of fixed effects as well as to retrieve accurate marginal effects of the predictors, making it ideal to use for the present study. Rainey and McCaskey (2021) further show that the Firth bias correction works reasonably well with small sample sizes and a small number of events. Nevertheless, to avoid problems

[4] In a reliability check, a second coder linked the terms to the identified labels. The overlap is 90 percent. The mismatch stems from economic topics that are harder to distinguish.

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

of over-fitting and saturation that can lead to biased estimates, the models were run separately for each topic.[5] The following statistical model was set up with the occurrence of a DoS attack as the dependent variable:

$$\text{Log}it(\text{DoS}_{i,t}) = \beta_0 + \beta_1 \text{topic}_{i,\,t} + \beta_2 \text{DoS}_{i,\,t-1} + \gamma_i + \delta_t + \epsilon_{i,t}, \tag{1}$$

where $\text{DoS}_{i,\ t-1}$ is a lagged dependent variable to control for serial correlation, γ_i includes newspaper fixed effects, δ_t day fixed effects and $\epsilon_{i,t}$ represents the error term. All models are run with newspaper-clustered standard errors.

Newspaper fixed effects were included as the nature of the news website influences whether it is attacked and its news reporting. By this, I further controlled for different levels of DoS protection, server capabilities, and the number of news headlines per website. Day fixed effects were added since temporal events have an impact on what is being reported and may also directly influence the likelihood of DoS attacks, e.g., proximity to elections (Lutscher *et al*., 2020).[6] From a theoretical viewpoint, the inclusion of both makes the most sense as the reporting on news content and the occurrence of DoS attacks are dependent on the newspaper and temporal developments. Nevertheless, the two-way fixed effects models assume that no idiosyncratic factor is influencing both—newspaper reporting and DoS attacks occurring at a specific point in time.

These models were run for every topic since outlets report on several news headlines per day and it could be, in theory, any headline or news topic that is responsible for a DoS attack being perpetrated. By running models for each topic, I can investigate whether the theoretically hypothesized topics are positively related to an increase in DoS attacks *and* if other topics do not show a positive relationship. To avoid that the results are driven by multiple comparisons, I adjust my analysis using the Bonferroni correction to avoid false positives (type I errors) as follows:

$$\alpha = \frac{0.05}{281} \tag{2}$$

where 0.05 is the conventional 5 percent significance level and 281 the number of models, including sensitivity tests, I run. Finally, since some topics and websites display high levels of collinearity, these topics are removed from the main analysis (see Table III and Online Appendix E for more details).

4. Analysis

To generate a bird's eye view, the 50 generated topics are ordered in the theoretically hypothesized broader topics that may increase the likelihood of DoS attacks, protest and repression (protest/repression), socioeconomic mismanagement (social/economic crisis), and regime delegitimizing topics (political legitimacy). The remaining topics were sorted into the categories of domestic politics, international politics, or nonpolitical topics. While the manual clustering of the different topics is explained in detail in Online Appendix C, I mainly relied on the news coverage of the topic, case knowledge, and between-topic correlations for this categorization.[7]

The aggregated results in Table III show the highest shares of significant positively-related topics in the repression/protest and legitimacy categories, whereas not as many significant topics

[5] Running models including all topics and fixed effects do not converge.

[6] To improve convergence and efficiency, I follow Cook *et al.* (2020) and only add dummies for days that experienced a DoS attack. To control for different topic proportions resulting from a diverging number of headlines per website, I include dummies for every news outlet.

[7] As a note of caution, the categorization is not necessarily exclusive for all topics.

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

Table 3. Categorization of topics

Category	$P(z)$	Topics	Share of pos. related topics ($\alpha = \frac{0.05}{281}$)
Social/economic crisis	0.311	Sanctions, migration crisis, petroleum, salary/prices, shortages healthcare, exchange rate, shortages, outages, **child mortality**, **PDVSA**, airline (opening/closing), indigenous groups/diseases, mining/sport (mixed), [recession], [work opinion], [economy opinion], [investment], [financial market], [investment/ infrastructure]	16.7 percent
Domestic politics	0.213	General opinion, **Maduro**, government-opposition dialog, government ministers, regulations, [economy policy], [food policy], [cryptomoney], [Spanish development aid]	20.0 percent
Political legitimacy	0.212	**National assembly**, opposition candidate, **election**, international organizations, **resignations**, corruption, **exiled opposition**, [leftist opposition]	57.1 percent
Protest/ repression	0.097	**Protest/shortages**, **Oscar Perez/repression**, **political prisoners**, military	75.0 percent
International politics	0.088	USA/Korea, Colombia border, **Cuba**, Russia, court sentences/Lula da Silva	20.0 percent
Nonpolitical topics	0.079	Earthquake/accidents, music/entertainment, church/job offer (mixed), education studies, [weather]	0.0 percent

Note: $P(z)$ = distribution over whole corpus. Topics within square brackets highly correlate to specific websites ($r \geq 0.6$) or did not converge and are excluded from the analysis. Bold topics display significant positive correlations.

appear in the social/economic crisis category. Concerning other categories, the analysis also reveals some patterns related to topics about international and domestic politics, whereas no relationship is found with topics that are clearly non-political. The statistical analysis thus provides overall support for Hypothesis 1 and Hypothesis 3 that expect a higher likelihood of DoS attacks when news outlets report on protests and repression or topics that question the regime's legitimacy.

To investigate this finding in greater detail, the average marginal effects (AMEs) were simulated for topics that display significant and positive associations. The panels in Figure 2 display these AMEs sorted into the broader categories and combined in one graph. The simulations display the "effect" of moving the share of the respective topic from its minimum to maximum value, i.e., reporting nothing at all to reporting extensively about the topic. In visualizing uncertainty levels, the figure reports the more conservative Bonferroni-corrected and unadjusted 95 percent confidence intervals.[8] All regression results are summarized in Online Appendix B.

Figure 2 shows that topics within the protest/repression category are associated with an increase of up to 13 percent in the likelihood of DoS attacks. This finding comes, however, with more uncertainty when considering the more conservative Bonferroni-corrected confidence intervals. In the social/economic crisis category, the AMEs are slightly smaller and only one topic —news about the government-owned oil company, *Petróleos de Venezuela S.A.* (PDVSA)—shows a robust association.

In the legitimacy category, the topics *resignations*, *exiled opposition*, and *election* display robust and, particularly for the two former topics, relatively large AMEs. The topic *exiled opposition* is primarily concerned with Antonio Ledezma, the ex-mayor of Caracas and former political prisoner, who constantly urges other governments to take action against the Maduro government. The topic *resignations* deals with the resignations of other heads of states and resignation demands pertaining to Maduro by domestic and international actors. Finally, the topic *national assembly*, which mainly reports on the opposition-filled *Asamblea Nacional* in 2017/18, shows a

[8] Bonferroni-corrected confidence intervals are calculated as follows: $1 - \frac{0.05}{281}$.

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

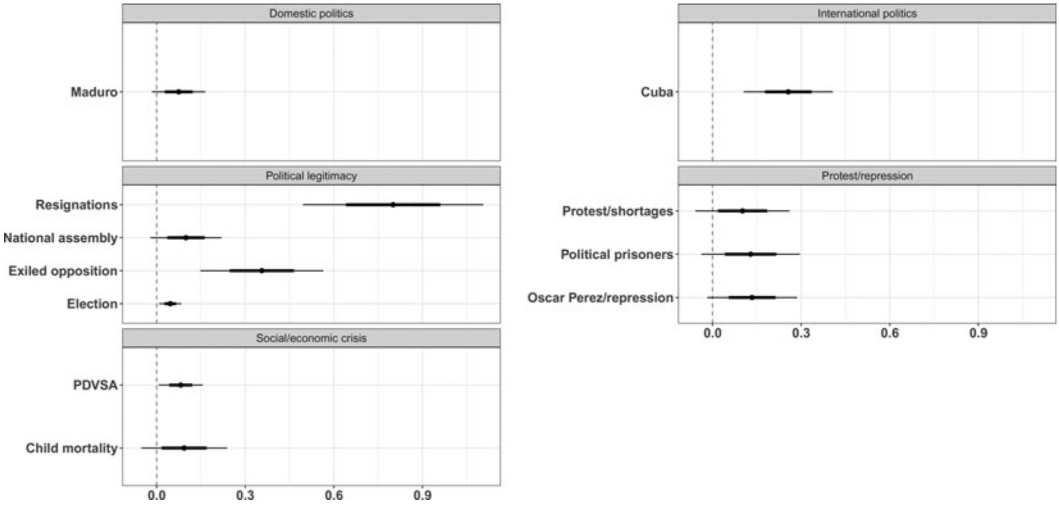

Fig. 2. Average marginal effects (AME) of significant positively-related topics on a news website's likelihood of receiving DoS attacks. Note: Each AME is calculated in separate models. Simulations based on 1000 draws. Topics are calculated in individual models and combined in the figure. Bonferroni-corrected (thin lines) and unadjusted (bold lines) 95 percent confidence intervals are displayed.

likewise positive association, yet misses conventional levels of statistical significance when considering the Bonferroni correction.

Surprisingly, news on *Cuba* also shows a relatively large and robust marginal effect. It might be that newspapers are attacked when criticizing the Venezuelan ally, Cuba, or wrote about the country's deviation from the "Cuban path" under the Maduro regime. A qualitative investigation of the leftist *Aporrea* outlet indeed shows that articles on the latter were published in February 2018, during a period when it was hit by several attacks. Reporting on this topic may thus implicitly undermine the political legitimacy of the Maduro regime. Finally, reporting on the relatively broad topic *Maduro* is also, albeit with higher levels of uncertainty, associated with an increased likelihood of DoS attacks.

Overall, these simulations lend the most support for Hypothesis 3 that expects a higher likelihood of DoS attacks when news outlets report on regime-delegitimizing topics. Yet, the analysis finds no relationship with the topic *opposition candidate*, which reports on the opposition candidates who run against Maduro in the presidential election or the topic *corruption*, for which it would be expected to see a positive correlation to DoS attacks. One likely explanation is that the opposition candidates who ran in the presidential elections were just not threatening enough. In fact, as mentioned in the case description, the more credible opposition figureheads Henrique Capriles, Leopold Lopez, and Antonio Ledezma were not allowed to run. Concerning corruption, this topic reports primarily on a state-led corruption investigation against former PDVSA officials and thus appears not to be censor-worthy from a government perspective.[9]

In Online Appendix D, I outline several additional tests conducted to investigate the robustness and sensitivity of the results. I ran permutation tests, controlled for legitimate traffic, considered single 503-error codes as DoS attacks, operationalized the topics differently, display negative related topics, and ran models considering previous reporting.[10]

[9] For the topic *international organizations* analyses examining previous reporting find some significant patterns (see Online Appendix D). Finally, while these results show that content seems to matter, this does not mean that the outlet *per se* is not important. Figure B.1 in Online Appendix B shows that the AMEs for specific newspapers range up to a 4.8 percent increase in the likelihood of DoS attacks.

[10] Due to the article's word limit, these tests had to be relegated to the supplementary material.

5. Discussion and limitations

What do these results tell us about the use of DoS attacks as a censorship tool against news outlets in autocracies? The presented main and the additional analyses in Online Appendix D could overall find support for my theoretical considerations. The results show, in particular, that regime-delegitimizing topics and news concerned with protests and repression are related to an increased likelihood of DoS attacks. These findings suggest that the Venezuelan government or state-related proxies are more likely to use DoS attacks to increase friction costs for users and news websites when outlets report on the above mentioned topics. Nevertheless, some important caveats remain.

First, while my research design and empirical analyses offer confidence that my measurement is capturing DoS attacks, I still infer these attacks from the retrieved error codes alone and unable to directly measure such attacks. Yet, if all measured 503-error codes had been by chance, we would not expect to see such clear relationships between the identified censor-worthy topics and the measurement. Another related limitation is that, apart from also measuring attack attempts against Cloudflare-protected servers, my measurement can capture successful attacks only.[11] Since for successful attacks more resources are needed, it is, however, more likely that these were purposely conducted. Future research should aim to solve these shortcomings by working together with news websites to gain access to their log data or find other ways to measure DoS attacks (e.g., Krupp *et al*., 2016).[12]

Second, another limitation is that it is difficult to link the reporting of specific headlines to one specific DoS attack event. The reason for this limitation is that a DoS attack affects the complete website and news outlets report on several headlines per day. By relying on the topic modeling approach together with the two-way fixed penalized models, I could determine what topics are associated with an increased likelihood of DoS attacks but not what exact headline is likely responsible for an attack. Future research could attempt to come up with better strategies on how to link specific headlines and DoS attacks.

Third, an inherent problem in studying DoS attacks remains their attribution. Given that such attacks are relatively simple to employ, other actors such as patriotic hackers may use these attacks against independent news outlets (Deibert *et al*., 2012). Pro-government or other groups may use DoS attacks against newspapers to punish them for their reports and thus signal discontent. This displeasure mechanism can be viewed as an emotional response by individuals or groups upset about the published content. Finally, government actors or their proxies may also use DoS attacks in an attempt to spread fear and intimidate outlets (cf. Roberts, 2018). Experiments show indeed that cyberattacks increase the individual's feelings of vulnerability and stress (Gross *et al*., 2017).[13]

6. Conclusion

By monitoring Venezuelan news outlets for seven months from November 2017 until June 2018, this paper offers new insights for the use of DoS attacks on news outlets in autocracies. My statistical analysis found several topics related to a higher likelihood of DoS attacks, where most topics either seem

[11] In Table D.6 provided in Online Appendix D, the prevalence of topics on attack days is compared between Cloudflare-protected and unprotected servers. The comparison shows no higher average reporting for any topic in the unprotected sample, suggesting that I have captured most DoS attacks on these servers.

[12] After the period of study, I contacted all of the studied websites and asked whether they experienced DoS attacks or attempts thereof. Although I reached out three times, only a few responded. This may perhaps be explained by the tense political situation in Venezuela, or because websites do not want to admit that they have been targeted as they come with reputation costs. Those websites that answered either stated that they were not attacked, confirming the patterns in the data, or highlighted that DoS attacks and other forms of censorship are commonly used against news websites in Venezuela (Email conversations; anonymized copies available upon request).

[13] Although DoS attacks are also often used by criminal actors, it is unclear why politically-sensitive content should trigger DoS for this purpose.

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

to question the political legitimacy of the regime or report on protests and repression. By establishing these relationships, my study provides further evidence on how authoritarian regimes use modern technologies to increase information friction beyond the widely-studied case of China (e.g., King *et al.*, 2013; Roberts, 2018; Gueorguiev and Malesky, 2019). In an electoral autocracy, it seems that not only protest and repression events are censor-worthy but also reports on the opposition and other topics that challenge the regime's political legitimacy.

Although this study comes with limitations related to the measurement and attribution of DoS attacks, the analysis is able to show relatively clear and non-random patterns concerning the relationship between specific news content and the likelihood of DoS attacks. Future work could build upon this paper and try out alternative measurement approaches or find ways how to attribute DoS attacks to specific actors (e.g., Krupp *et al.*, 2016). Such an advancement would also allow for a more detailed exploration of the mechanisms introduced by this paper. Moreover, to understand how generalizable these results are, future research should investigate the use of DoS attacks on news outlets from a cross-national perspective. Finally, an important next endeavor will be to quantify the consequences of DoS attacks and other censoring tools for news outlets.

While the Internet has made it easier for the press to circumvent censorship, my study could show that news outlets are still vulnerable to censorship in the digital age. Whereas the ability of authoritarian governments to control information has been often limited by their borders in the past, modern-day authoritarian regimes can use cyberattacks and other digital means to globally censor and suppress opposition voices. While my study gives some hope that DoS attacks are not as widely used for this purpose, authoritarian regimes rely increasingly on a combination of different tools including DoS attacks, website filters, and social media flooding to control their online spheres (e.g., King *et al.*, 2013; Munger *et al.*, 2018; Roberts, 2018; Sanovich *et al.*, 2018; Morales, 2019).

Supplementary material. The supplementary material for this article can be found at https://doi.org/10.1017/psrm.2021.68. To obtain replication material for this article, please visit https://doi.org/10.7910/DVN/AK1C65

Acknowledgments. I am very grateful to Nils B. Weidmann and Karsten Donnay, as well as Molly Roberts who supported me from the early stages of this project. Moreover, Sebastian Hellmeier and Max Heermann have provided extremely helpful comments on this project. I am furthermore indebted to Sebastian Schutte and Carl Henrik Knutsen for their essential feedback when preparing this manuscript. In addition, I would like to thank participants of the 2018 AFK method and data workshop at the GIGA in Hamburg, the 2018 IMAPS workshop at the USCD, San Diego, the 2019 QTA-DUB workshop at the UCD in Dublin, and the 2019 EPSA conference in Belfast, in particular, Constantine Boussalis and Aseynur Dal. Finally, I thank the two anonymous reviewers and the editor of PSRM, Nils Metternich, whose comments led to major improvements of this paper. This work was supported by the University of Konstanz, the German National Science Foundation (#402127652), and the European Research Council (#863486). All remaining errors are my own.

References

Aporrea (2021) Sepa Cómo Evadir El Bloqueo a Aporrea.org En Los Proveedores de Internet del Estado Venezolano. *Aporrea*, March 14. https://www.aporrea.org/medios/n363477.html (accessed 05-03-2021).

Athey S and Mobius M (2012) The impact of news aggregators on internet news consumption: the case of localization. Working Paper. Harvard University and Iowa State University.

BBC, Worldwide Monitoring (2009) Leading Russian newspaper reports attack on its website. December 16. https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:7XBB-55K1-2R51-70WR-00000-00&context=1516831 (accessed 07-29-2019).

Brutlag J (2009) Speed matters for Google web search. *Google*. https://services.google.com/fh/files/blogs/google_delayexp.pdf (accessed 07-29-2019).

Cardenas, Cat. (2017) Freedom of the press also targeted virtually in Venezuela, where cyberattacks can force independent sites offline. *Journalism in the Americas*. https://knightcenter.utexas.edu/blog/00-18194-freedom-press-also-targeted-virtually-venezuela-where-cyberattacks-can-force-independe (accessed 07-29-2019).

Cloudflare (2020) Understanding Cloudflare under attack-mode advanced DDOS protection. https://support.cloudflare.com/hc/en-us/articles/200170076-Understanding-Cloudflare-Under-Attack-mode-advanced-DDOS-protection-.

Cook SJ, Hays JC and Franzese RJ (2020) Fixed effects in rare events data: a penalized maximum likelihood solution. *Political Science Research and Methods* **8**, 92–105.

Deibert R, Palfrey J, Rohozinski R, Zittrain J and Gross JC (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Boston: MIT Press.

Deibert RJ, Rohozinski R and Crete-Nishihata M (2012) Cyclones in cyberspace: information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue* **43**, 3–24.

Dorsch MT, Dunz K and Maarek P (2015) Macro shocks and costly political action in non-democracies. *Public Choice* **162**, 381–404.

Edmond C (2013) Information manipulation, coordination, and regime change. *Review of Economic Studies* **80**, 1422–1458.

Firth D (1993) Bias reduction of maximum likelihood estimates. *Biometrika* **80**, 27–38.

Franceschi-Bicchierai L (2019) Venezuela's government appears to be trying to hack activists with phishing pages. *Vice*, February 15. https://www.vice.com/en_us/article/d3mdxm/venezuela-government-hack-activists-phishing (accessed 04-22-2020).

Freedom House (2016) Freedom of the Net 2016: silencing the messenger: communication apps under pressure. Washington, DC: Freedom House.

Freedom House (2017*a*) Freedom of the Press 2017: press freedom's dark horizon. Washington, DC: Freedom House.

Freedom House (2017*b*) Freedom on the Net 2017: manipulating social media to undermine democracy. Washington, DC.: Freedom House.

Galicia Lugo H (2019) FANB activó protocolos ante hackers mientras ataca a portales de medios de comunicación. https://cronica.uno/fanb-activo-protocolos-ante-hackers-mientras-ataca-a-portales-de-medios-de-comunicacion/.

Gehlbach S and Sonin K (2014) Government control of the media. *Journal of Public Economics* **118**, 163–171.

Global Voices (2011) Russia: election day DDoS-alypse. https://globalvoices.org/2011/12/05/russia-election-day-ddos-alypse/print/ (accessed 07-29-2019).

Grimmer J and Stewart BM (2013) Text as data: the promise and pitfalls of automatic content analysis methods for political texts. *Political Analysis* **21**, 267–297.

Gross ML, Canetti D and Vashdi DR (2017) Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity* **3**, 49–58.

Gueorguiev DD and Malesky EJ (2019) Consultation and selective censorship in China. *The Journal of Politics* **81**, 1539–1545.

Guriev S and Treisman D (2019) Informational autocrats. *Journal of Economic Perspectives* **33**, 100–127.

Hardy S, Crete-Nishihata M, Kleemola K, Senft A, Sonne B, Wiseman G, Gill P and Deibert RJ (2014) Targeted threat index: characterizing and quantifying politically-motivated targeted malware. In *23rd USENIX Security Symposium (USENIX Security 14),* Program chair: Kevin Fu. San Diego, CA: USENIX Association, pp. 527–541.

Hawkins KA (2016) Chavismo, liberal democracy, and radical democracy. *Annual Review of Political Science* **19**, 311–329.

Hellmeier S (2016) The dictator's digital toolkit: explaining variation in internet filtering in authoritarian regimes. *Politics & Policy* **44**, 1158–1191.

Herrero AV and Semple K (2018) Venezuela opposition will boycott election, and Maduro tightens his hold. *New York Times*, Feb 21. https://www.nytimes.com/2018/02/21/world/americas/venezuela-election-opposition-boycott.html (accessed 05-03-2021).

IPYS, Instituto Prensa y Sociedad Venezuela (2017) Aporrea Sufrió Ataque Cibernético Masivo. https://ooni.torproject.org/post/venezuela-internet-censorship/ (accessed 10-26-2020).

Jagannathan M (2012) DDoS attacks disable independent news sites during Russian protests. https://blogs.harvard.edu/herdict/2012/06/14/ddos-attacks-disable-independent-news-sites-during-russian-protests/ (accessed 2019-07-29).

Jonker M, King A, Krupp J, Rossow C, Sperotto A and Dainotti A (2017) Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In *Proceedings of the 2017 Internet Measurement Conference,* Chairs of conference: Steve Uhlig and Olaf Maennel. IMC '17 New York, NY, USA: ACM. pp. 100–113.

King G, Pan J and Roberts ME (2013) How censorship in China allows government criticism but silences collective expression. *American Political Science Review* **107**, 1–18.

King G, Pan J and Roberts ME (2017) How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review* **111**, 484–501.

Klyueva A (2016) Taming online political engagement in Russia: disempowered publics, empowered state and challenges of the fully functioning society. *International Journal of Communication* **10**, 20.

Krupp J, Backes M and Rossow C (2016) Identifying the scan and attack infrastructures behind amplification DDoS attacks. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* Program chairs: Edgar Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew Myers, Shai Halevi. New York, NY, USA; Vienna, Austria: Association for Computing Machinery. pp. 1426–1437.

La Patilla (2018*a*) CANTV Continúa el Bloqueo a La Patilla. *La Patilla*, August 24. https://www.lapatilla.com/2018/08/24/cantv-continua-el-bloqueo-a-la-patilla/.

La Patilla (2018*b*) SIP advierte sobre ataques cibernéticos del gobierno contra La Patilla. *La Patilla*, October 20. https://www.lapatilla.com/2018/10/20/sip-advierte-sobre-ataques-ciberneticos-del-gobierno-contra-la-patilla/ (accessed 04-03-2020).

https://doi.org/10.1017/psrm.2021.68 Published online by Cambridge University Press

Lutscher PM, Weidmann NB, Roberts ME, Jonker M, King A and Dainotti A (2020) At home and abroad: the use of denial-of-service attacks during elections in nondemocratic regimes. *Journal of Conflict Resolution* **64**, 1–29.

Martin B (2007) *Justice ignited: the dynamics of backfire*. Lanham, MD: Rowman & Littlefield.

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

Mitchelstein E and Boczkowski PJ (2009) Between tradition and change: a review of recent research on online news production. *Journalism* **10**, 562–586.

Morales JS (2019) Perceived popularity and online political dissent: evidence from Twitter in Venezuela. *The International Journal of Press/Politics* **25**, 5–27.

Munger K, Bonneau R, Nagler J and Tucker JA (2018) Elites tweet to get feet off the streets: measuring regime social media strategies during protest. *Political Science Research and Methods* **7**, 815–834.

Nazario J (2009) Politically motivated denial of service attacks. In Christian C and Kenneth G (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam/Washington, DC: IOS Press, pp. 163–181.

OONI, Open Observatory of Network Interference (2018) The state of internet censorship in Venezuela. https://ooni.torproject.org/post/venezuela-internet-censorship/ (accessed 07-30-2019).

Pan J and Siegel AA (2020) How Saudi crackdowns fail to silence online dissent. *American Political Science Review* **114**, 109–125.

Pearce KE and Kendzior S (2012) Networked authoritarianism and social media in Azerbaijan. *Journal of Communication* **62**, 283–298.

Pearce P, Jones B, Li F, Ensafi R, Feamster N, Weaver N and Paxson V (2017) Global measurement of DNS manipulation. In *26th USENIX Security Symposium (USENIX Security 17),* Program chairs: Engin Kirda and Thomas Ristenpart. Vancouver, BC: USENIX Association. pp. 307–323.

Rainey C and McCaskey K (2021) Estimating logit models with small samples. *Political Science Research and Methods* **Online First**, 1–16.

Rasler K (1996) Concessions, repression, and political protest in the Iranian revolution. *American Sociological Review* **61**, 132–152.

Richter P, Padmanabhan R, Spring N, Berger A and Clark D (2018) Advancing the art of internet edge outage detection. In *Proceedings of the Internet Measurement Conference 2018*. IMC '18 New York, NY: ACM, pp. 350–363.

Roberts ME (2018) *Censored: Distraction and Diversion Inside Chinas Great Firewall*. Princeton, NJ: Princeton University Press.

Rosas R (2019) Atacan Servidores de Efecto Cocuyo, El Pitazo y El Cooperante y CANTV Bloquea Twitter y Soundcloud. *Efecto Cocuyo*, March 04. http://efectococuyo.com/principales/atacan-servidores-de-efecto-cocuyo-el-pitazo-y-el-cooperante-y-cantv-bloquea-twitter-y-soundcloud/ (accessed 07-30-2019).

Rozenas A and Stukal D (2019) How autocrats manipulate economic news: evidence from Russia's state-controlled television. *The Journal of Politics* **81**, 982–996.

Rueda M (2015) Coordinated DDoS attack during Russian duma elections. *Splinter*, June 23, note = https://splinternews.com/meet-the-venezuelan-rebel-whose-crime-is-publishing-exc-1793848615 (accessed 03-24-2020).

Sanovich S, Stukal D and Tucker JA (2018) Turning the virtual tables: government strategies for addressing online opposition with an application to Russia. *Comparative Politics* **50**, 435–482.

Sen AK (2018) Venezuela's Sham election. *Atlantic Council*. http://www.atlanticcouncil.org/blogs/new-atlanticist/venezuelas-sham-election (accessed 07-30-2019).

Spaiser V, Chadefaux T, Donnay K, Russmann F and Helbing D (2017) Communication power struggles on social media: a case study of the 2011–12 Russian protests. *Journal of Information Technology & Politics* **14**, 132–153.

Stier S (2015) Democracy, autocracy and the mews: the impact of regime type on media freedom. *Democratization* **22**, 1273–1295.

Svolik M (2012) *The Politics of Authoritarian Rule*. Cambridge: Cambridge University Press.

The Turkish Newswire (2014) Most companies vulnerable to cyber threat, report says. *The Turkish Newswire*, April 04. https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5BWN-T3V1-DXCW-D39S-00000-00&context=1516831 (accessed 08-06-2019).

Tucker JA (2007) Enough! Electoral fraud, collective action problems, and post-communist colored revolutions. *Perspectives on Politics* **5**, 535–551.

Walker HA, Rogers L and Zelditch M Jr. (1988) Legitimacy and collective action: a research note. *Social Forces* **67**, 216–228.

Xu X (2020) To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science* **65**, 309–303.

Yan X, Guo J, Lan Y and Cheng X (2013) A biterm topic model for short texts. In *Proceedings of the 22nd International Conference on World Wide Web*. WWW '13 New York, NY, USA: ACM, pp. 1445–1456.

Cite this article: Lutscher PM (2023). Hot topics: Denial-of-Service attacks on news websites in autocracies. *Political Science Research and Methods* **11**, 696–711. https://doi.org/10.1017/psrm.2021.68