Censor & Contend:

The Use of Denial-of-Service Attacks in Autocracies

Dissertation submitted for the degree of
Doctor of Social Sciences (Dr.rer.soc.)

presented by

Philipp Matthias Lutscher

at

Universität Konstanz

Sektion Politik - Recht - Wirtschaft

Fachbereich Politik & Verwaltungswissenschaft

Konstanz, 2020

Date of defense:	January 27, 2020
First Referee:	Prof. Dr. Nils B. Weidmann
Second Referee:	Jun.-Prof. Dr. Karsten Donnay
Third Referee:	Prof. Margaret E. Roberts

Für Kurt, ich vermisse dich.
Para Catalina, te amo.

Acknowledgments

Writing this dissertation would not have been possible with the support and encouragement of various people.

Foremost, I would like to thank my main supervisor Nils Weidmann. When I was still an undergraduate student, it was he who sparked my interest in doing research. Since then, Nils has supported me greatly in my journey of becoming a political scientist. I am very grateful for his often challenging but valuable feedback, research and traveling funding, network and collaboration, as well as general mentoring.

Second, I would like to thank my two other supervisors Karsten Donnay and Molly Roberts. Karsten had always time for me and encouraged me constantly to improve my papers. With Molly, I had the opportunity to co-author a paper in an international and interdisciplinary team where I learned a lot. In that regard, I would also like to thank Alberto Dainotti and Alistair King from the Center of Advanced Internet Data Analysis, as well as Mattijis Jonker, for our fruitful collaboration. Their data collection on Denial-of-Service attacks made most of the empirical analysis in this dissertation possible in the first place.

Apart from my supervisors and co-authors, my fantastic colleagues read, commented, and helped to improve much of my dissertation's papers. Big thanks to Sebastian, Eda, Lukas, Annerose, Espen, as well as especially Max, who had the pleasure of reading most of my work. Also, a big thanks to Philipp for his language support. Besides, discussions with other students, post-docs, and professors from the department and Graduate School of Decision Sciences (GSDS) improved my papers a lot. Here, I would like to mention, in particular, Basti, Julian, Peter, Clara, Patrick, Roman, Constantin, Philipp and Carlo. Beyond Konstanz, I would like to thank Tina Freyburg and Anita Gohdes for their invitations to workshops and conference panels as well as their valuable comments.

Furthermore, thanks to the GSDS, the German Research Foundation, and the "The Politics of Inequality" cluster of excellence that funded me. I am very thankful to these organizations and employers for supporting my research. Besides, without the support of the Friedrich Ebert Stiftung during my undergraduate and graduate studies, I probably would not have made it that far as a first-generation scholar.

Finally, I would like to thank my family. Thanks to my parents for their lifelong support and understanding that I have to go my own way. Most importantly, thank you, Catalina. I am incredibly grateful for your unconditional support, patience, motivational speeches and more. *Juntos movemos montañas.*

Zusammenfassung

In den letzten Jahren wurden Cyberangriffe stark in den Medien, der Politik und der Wissenschaft diskutiert. In dieser Dissertation untersuche ich die politische Verwendung einer speziellen Art von Cyberangriffen, den so genannte "Denial-of-Service" (DoS) Angriff. Diese relativ einfache Art von Angriff überladt Server mit Internet-Datenströmen, was zu einem temporären Nichterreichen des attackierten Servers führt. Die größte öffentliche und akademische Aufmerksamkeit erhielten politisch motivierte DoS Angriffe im Zusammenhang mit zwischenstaatlichen Konflikten. In dieser Dissertation zeige ich hingegen, dass in Autokratien hauptsächlich innerstaatliche Gründe für die politische Verwendung von DoS Angriffen verantwortlich sind.

Hierfür verknüpfe ich Literatur aus den Forschungsfelder der Sozialen Bewegungen, der Autokratischen Politik und den Internationalen Beziehungen und formuliere zwei theoretische Hauptmechanismen für die politische Verwendung von DoS Angriffen in Autokratien. Diese werden zur Zensur von Webseiten verwendet oder, um gegen die Regierungspolitik des eigenen Landes oder fremder Staaten zu protestieren. Im empirischen Teil meiner Dissertation verwende ich zwei neue Datenquelle zur Messung von DoS Angriffen. Die erste Datenquelle kommt von dem "Center for Advanced Internet Analysis" (CAIDA) an der University of California, San Diego, welche DoS Angriffe aus Internet-Datenströmen misst. Die zweite Datenquelle beruht auf einer eigenen Messung von Nachrichtenwebseiten in autokratischen Ländern, in der ich Webseitenstatusabfragen verwende, um auf DoS Angriffe zu schließen.

Im ersten Papier, das gemeinsam mit Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King und Alberto Dainotti verfasst ist, fragen wir, ob innerstaatliche Ereignisse die Wahrscheinlichkeit von DoS Angriffen erhöhen. Hierzu untersuchen wir in einer weltweiten Studie, ob diese Angriffe während Wahlperioden zwischen 2008 und 2016 zunehmen. Die theoretische Erwartung ist, dass die Anzahl von DoS Angriffen insbesondere in Autokratien zunehmen sollte, da hier sowohl autokratische Regierungen als auch Aktivisten Anreize haben diese zu nutzen. In der empirischen Analyse verwenden wir die oben erwähnten Daten von CAIDA und zeigen, dass Wahlperioden positiv mit der Anzahl von DoS Angriffen korrelieren. Diese positive Korrelation ist jedoch nicht unbedingt für Angriffe auf das autokratischen Land sichtbar, sondern auf Server in Staaten in denen Nachrichtenwebseiten für die jeweilige Autokratie gehostet sind. Zusammengefasst deutet unsere Studie darauf hin, dass autokratische Regierungen DoS Angriffe gegen Server im Ausland verwenden und über ihre Grenzen hinweg zensieren.

Im zweiten Papier untersuche ich die Zensurfunktion von DoS Angriffen genauer und fokussiere mich auf die Gründe und den Zeitpunkt von DoS Angriffen auf Webseiten. Hierfür überwache ich einige Nachrichtenwebseiten in Venezuela von November 2017 bis Juni 2018. Ich argumentiere, dass DoS Angriffe auf Nachrichtenwebseiten verwendet werden, um Informationen temporär zu zensieren, aber auch, um repressive Signale an Zeitungen zu senden. Im empirischen Teil untersuche ich ob das Berichten über sensitive Themen die Wahrscheinlichkeit auf Nachrichtenseiten von DoS Angriffen kurz- und mittelfristig erhöht. Aus dem Grund, dass es im Vorhinein nicht eindeutig ist, welche Nachrichten für die Regierung sensitiv sind, verwende ich "topic modeling" Ansätze, welche induktiv herauszufinden über welche Themen venezolanische Nachrichtenseiten berichten. Die Ergebnisse zeigen Evidenz für beide Mechanismen, jedoch scheint die repressive Verwendung von DoS Angriffen auf Zeitungen ausgeprägter zu sein.

Im dritten Papier überdenke ich die Behauptung vieler Kommentatoren von einem

Cyberkrieg zwischen Nationen, indem ich untersuche ob DoS Angriffe als Drohmittel verwendet werden. Hierzu fokussiere ich mich auf Wirtschaftssanktionen, bei denen man eine digitale Antwort von sanktionierten Ländern erwarten kann. Ich schlage zwei Mechanismen vor warum dies der Fall sein könnte. Erstens könnten Staaten mit DoS Angriffen rational auf Sanktionsandrohungen und -verhängungen reagieren, um Zugeständnisse zu erreichen. Zweitens könnten Regierungen und Gruppen innerhalb sanktionierter Staaten mit DoS Angriffe als Protestmittel antworten. Für den empirischen Teil verwende ich wiederum die Daten von CAIDA und Zeitreihenanalysen. Die Ergebnisse zeigen keine Evidenz für einen Anstieg von DoS Angriffen auf das Senderland nach Sanktionsdrohungen und nur in ein paar Fällen einen signifikanten Anstieg nach Sanktionsverhängungen. Diese Ergebnisse ziehen die These, dass DoS Angriffe ein häufig genutztes Mittel von Regierungen für internationale Auseinandersetzungen sind, in Zweifel. Eine zuätzlichen Fallstudie legt nahe, dass etwaige DoS Angriffe in diesem Kontext eher als Protestmittel eingesetzt werden.

Zusammengefasst leistet meine Dissertation mindestens drei wichtige Beiträge zur bisherigen Forschung. Erstens zeige ich, dass DoS Angriffe in autokratischen Regimen für politische Zwecke verwendet werden und zwar insbesondere aus innerstaatlichen Gründen. Zweitens formuliere ich theoretische Erwartungen warum und wann bestimmte Akteure DoS Angriffe in Autokratien verwenden und finde hauptsächlich Anhaltspunkte für die Verwendung von DoS Angriffen als Zensurmittel. Schlussendlich verwende ich zwei neue Messungen von DoS Attacken, welche es erlauben, genauere empirische Analysen durchzufüren, um so ein umfassenderes Bild von Cyberaktivitäten zu zeichnen.

Abstract

In recent years, cyberwarfare has been a hotly debated issue. In this dissertation, I investigate the use of one particular type of cyberattacks: Denial-of-Service (DoS) attacks. These relatively simple attacks overload servers with Internet data traffic, making them temporally not reachable. Most of the public and academic attention has been on their use during interstate conflicts. Even so, in this dissertation, I show that in autocracies domestic reasons are primarily responsible for the political use of DoS attacks.

To explain the use of DoS attacks, I connect literature from three research fields: social movements, autocratic politics, and international relations. From this, I develop two main theoretical mechanisms for the political use of DoS attacks in autocracies. The latter are employed to censor threatening websites or to contend governmental policies of the own or other states. I rely on two new data sources that measure DoS attacks. The first comes from the Center for Advanced Internet Analysis (CAIDA) at the University of California, San Diego, measuring DoS attacks from Internet traffic data. The second is an own measurement for news websites in several authoritarian countries, where I query the websites' status codes to infer DoS attacks. Both the theoretical framework and new data sources represent a new and previously absent contribution to the study of cyberattacks.

In the first paper, which was jointly written with Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti, the goal is to explore whether politically domestic events increase the likelihood of DoS attacks. We investigate whether the number of DoS attacks increases during election periods from 2008 – 2016 worldwide. We expect that the frequency of DoS attacks rises especially in autocracies as here both governments and activists have incentives to employ them. Using the data on DoS attacks provided by CAIDA, we show that election periods in autocracies are positively associated with the number of DoS attacks. However, this increase is not necessarily visible on the autocracy itself but on foreign servers where country-related newspapers are hosted. In conclusion, our study suggests that authoritarian governments use DoS attacks to export censorship beyond their borders and attack servers abroad.

In the second paper, I investigate the censorship function of DoS attacks in greater detail and explore the reasons and timing for attacks on websites. For this, I monitor several news websites in Venezuela from November 2017 to June 2018. I argue that DoS attacks target news websites to censor sensitive information temporally, but also to send repressive signals to these media outlets. In the empirical part, I investigate these mechanisms by looking at whether reporting on specific news topics increase the likelihood of DoS attacks in the short- and medium-term. Since it is *a priori* unknown what news are sensitive, I employ topic modeling approaches to determine topics Venezuelan news websites report on. The results show evidence for both mechanisms. However, the use of DoS attacks on news websites as a repressive tool appears to be more pronounced.

In the third paper, I revisit the claim by many pundits about a cyberwar between nations and investigate a potential coercive use of DoS attacks. In this paper, I focus on liberal sanctions, where one can expect a digital response by targeted states. I propose two mechanisms of why this may be the case. First, states could respond to both sanction threats and impositions with DoS attacks to achieve concessions by the sender state. Second, governments and/or groups within targeted countries may launch DoS attacks to signal discontent. For the empirical part, I again use the data provided by CAIDA and time series models. The results do not show an increase of DoS attacks

against sender countries after sanction threats, and, only in a few cases, a significant increase after sanction impositions. These results question the use of DoS attacks as a widely employed coercive tool for interstate conflict. As supported by an additional case study, it is rather activists or patriotic hacking groups that may use them as a contentious response in this context.

In conclusion, my dissertation makes at least three important contributions to the previous literature. First, I show that DoS attacks are used in autocracies for political reasons and that especially domestic events appear to trigger them. Second, I develop theoretical explanations for why and when certain actors employ DoS attacks in autocracies, finding primarily evidence for a censorship use of DoS attacks. Finally, I use two new measurements of DoS attacks, allowing to conduct more accurate empirical analyses and to get a more comprehensive picture of cyber activities.

Contents

List of Figures

List of Tables

1 Introduction

In the last decades, the world has seen the most rapid technological revolution in humankind. Although information and communication technologies (ICTs) such as radio, television and phone technologies emerged already in the 20th century, the spread of personal computers, cellphones, and the Internet has changed economies, societies and politics profoundly. These modern ICTs enable users to not only receive but also to broadcast and to distribute information themselves. Social media is probably the prime example of this novel feature. In his essay "Liberation Technology" in 2010, Larry Diamond describes the Internet as a decentralized medium that can reach large numbers of people, ease communication and political mobilization, pluralize sources of information and help to hold the powerful accountable. While this view has been widely shared, other scholars emphasize the downside of modern technologies, particularly the Internet. With the Internet, it has become easier for governments to monitor and influence their population, to censor information, and to disrupt other countries, in particular in authoritarian systems (e.g., Morozov, 2011; MacKinnon, 2013; Roberts, 2018; Tucker et al., 2017; Valeriano and Maness, 2014).[1]

Research on the political effects of modern ICTs in autocracies has largely focused on how governments control content in the digital sphere. Studies show how governments selectively censor social media posts or influence virtual discussions, to name just these two examples (Deibert and Rohozinski, 2010; Gunitsky, 2015; King, Pan and Roberts,

[1]Clearly, these points are not only restricted to governments, but also non-state groups use the Internet for these and other purposes. For instance, scholarly work shows how groups use the Internet for radicalization purposes (e.g., Zeitzoff, 2017).

2013, 2017). In a similar vein, scholarly works on the use of modern ICTs by citizens and activists in authoritarian regimes primarily focus on the political communication aspect of these technologies (e.g., Diamond, 2010; Howard and Hussain, 2011; Enikolopov, Makarin and Petrova, 2018). Less research has explored how actors exploit the Internet's network structure for political purposes. For instance, there are some studies on the use of network outages in authoritarian countries (Howard, Agarwal and Hussain, 2011; Dainotti et al., 2014). However, political actors can also use more targeted ways to disable, disturb or infiltrate computer networks. These measures are often referred to as cyberattacks.

According to cyber security firms, cyberattacks are very common in today's connected world. Without a doubt, most of these attacks are non-political and launched by private actors, for example for criminal purposes (e.g., Netscout, 2017). Nevertheless, these tools are also open to political actors. Previous literature proposes numerous definitions for political cyberattacks. Many of these definitions are very narrow, focusing either on specific attack vectors, or making the requirement that nation-states have to be the perpetrator of these attacks (e.g., Richard, Robert et al., 2010). In this dissertation, I follow Hathaway et al. (2012) who state that "[a] cyberattack consists of any action taken to undermine the function of a computer network for a political or national security purposes." This definition does not only include all types of undermining attempts but also makes no requirements about a state involvement for these attacks. After all, as stated by pundits and shown in later examples especially relatively simple types of cyberattacks can be easily employed by non-state actors as well (e.g., Schmidt and Cohen, 2016).

One of these brute-force and simultaneously the most frequent type of cyberattacks are so-called Denial-of-Service (DoS) attacks. This particular form of cyberattack aims to temporally disable web services by flooding them with high levels of data traffic. While there are various attack vectors to achieve this, perpetrators often use several devices in so-called Distributed Denial-of-Service (DDoS) attacks together to generate enough data traffic on the victim server.[2]

Politically motivated DoS attacks during interstate disputes have probably received the most public and academic attention. Prominent examples for this use were DoS attacks against web servers in Estonia in 2007 or Georgia in 2008. In these cases, both countries suffered from large-scale DoS attacks on government, news and industry websites supposedly launched by Russian actors (Nazario, 2009; Valeriano and Maness, 2014). Less interest has been on domestic reasons for cyberattacks. On the one hand, examples show that activists and international politically motivated hackers use DoS attacks against government websites. For example, there are accounts of such attacks during the 2009 Iranian post-election "Green Revolution" (Beyer, 2014) or the Arab uprising

[2]From now on I will use the abbreviation DoS only that includes the use DDoS attacks. For an overview of other common DoS attack vectors (see, e.g., Netscout, 2017).

in 2011 (Coleman, 2014). On the other hand, there is ample anecdotal evidence for the use of DoS attacks by presumably authoritarian governments or government-related groups to silence independent news, human rights or opposition websites (e.g., Nazario, 2009; Zuckerman et al., 2010). For instance, during the 2011 election in Russia, various independent and critical news outlets were attacked and not reachable on the election day (Roberts and Etling, 2011). More recently, while several thousand citizens protested the extradition law in Hong Kong in 2019, the messenger service Telegram was hit by a large-scale DoS attack supposedly carried out by Chinese authorities (Shanapinda, 2019).

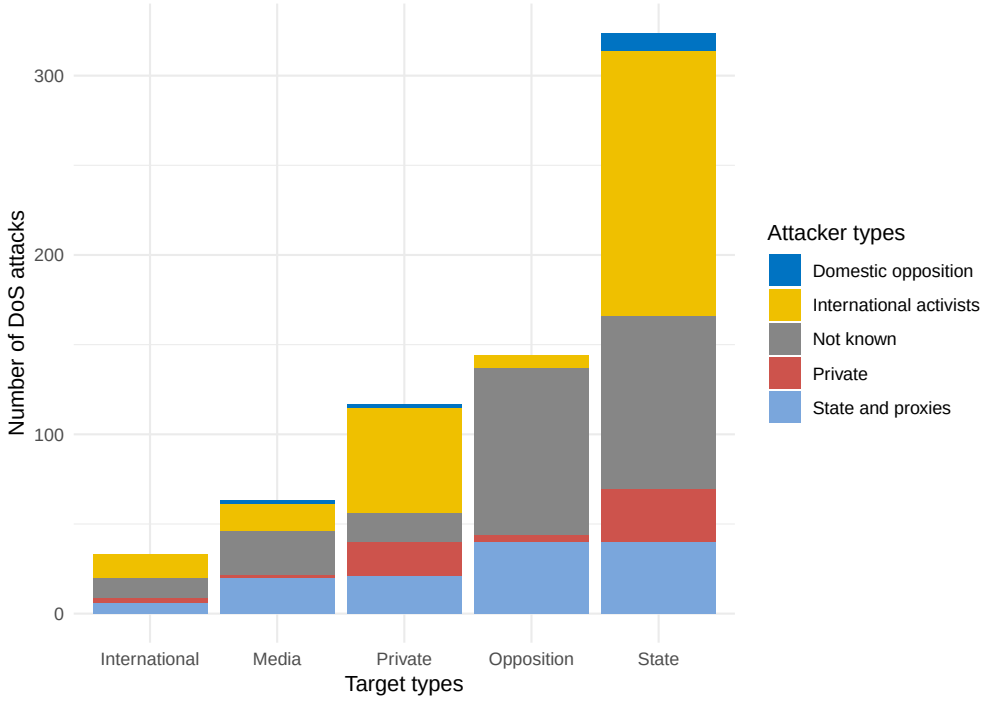

Figure 1.1: DoS attacks recorded by English-language newspapers 2008 - 2016. For more details on the collected data, refer to Appendix B.

A more systematic survey of politically motivated DoS attacks using newspaper reports reveals some interesting first patterns.[3] Although the majority of the recorded DoS attacks target government and government-related websites, most of them appear to be conducted by international activists. Besides, the data show that opposition actors (parties, critical newspapers, etc.) and media outlets (newspapers, blogs, and social media) are frequently targeted by politically motivated DoS attacks as well. Finally, Figure 1.1 highlights a considerable number of politically motivated DoS attacks on private targets (e.g., companies). Here, the data include reports about DoS attacks on

[3]In Appendix B, I present the codebook for this data collection, which I conducted with the help of student assistants within the scope of this dissertation. I hereby would like to thank Eke and Lea for their coding efforts.

PayPal in 2011 by the global Internet group *Anonymous* to protest company policies, for instance. Finally the data shows that activists also target Western companies and governments to protest against what they perceive as unfair policies. While these observations contradict the above stated prominent use of cyberattacks during interstate warfare, the interpretation of the just presented data may be heavily biased due to the reliance on media-based data. First, only public and for media outlets interesting DoS attacks are reported. Second, while some actors, most likely activists, want to claim DoS attacks, other actors rather have incentives to hide them. Finally, there appears to be also a clear bias towards English-speaking and geo-politically important countries (see subsection 1.1.4).

The focus of this work is on the use of DoS attacks in autocracies.[4] There are two main reasons for this. First, only authoritarian governments appear to use DoS attacks for the above-outlined censorship purposes. In contrast, democratic countries are (in most cases) heavily constrained by laws in their ability to use DoS attacks, in particular, when it comes to domestically motivated attacks. Second, channels of contention for citizens and activists are limited in authoritarian countries. DoS attacks might be thus a viable alternative to express discontent in these regimes. Finally, also the use of DoS attacks as an international tool to disrupt other countries appears to be more pronounced in autocracies.

In sum, the goal of this dissertation is to explore the motivation to launch DoS attacks in non-democratic countries and to offer empirical tests on this phenomenon. I argue that the main political uses of DoS attacks in authoritarian states are (1) to censor sensitive websites and content, and (2) to contend governmental policies of the own or other states. Contrary to the few empirical studies before, I do not use media-based data to investigate this question. Instead, I rely on Internet traffic data, and website status queries to infer DoS attacks. Thereby, my dissertation helps not only to advance our understanding of the political use of DoS attacks on a theoretical level but also paints a more comprehensive empirical picture of the use of DoS attacks in authoritarian states.

1.1 The Study of Digital Politics

Modern ICTs, in particular the Internet, have created new tools for citizens, activists, and government to influence politics. In this section I discuss three different fields of study that show how modern ICTs changed politics and how cyber- and DoS attacks are politically used. In the following, I first introduce the related literature from a social movement perspective. Second, I survey the literature from an authoritarian politics angle. Finally, I focus on the use of cyberattacks from an international relations

[4] In the definition of an authoritarian regime, I follow Geddes, Wright and Frantz (2014) and consider a regime as autocratic if the government, (1) came to power using "undemocratic" means (i.e., not through fair and free elections), (2) came to power through elections but changed the rules in their favor for future elections or (3) if the military stepped in.

perspective.

1.1.1 Previous Literature from a Social Movement Perspective

This subsection begins by introducing the broader literature on contentious politics and direct action and how the digital era transformed contentious behavior. Following from this, I present studies that focus on new forms of contention in the digital age, primarily DoS attacks. Finally, I discuss the few studies that aim to answer when these attacks are mounted and discuss the shortcomings of this branch of literature.

Tilly, McAdam and Tarrow (2001) defines contentious politics as an irregular, public, and collective interaction among makers of claims. In most cases, this refers to a collective political struggle, normally between powerless groups and more powerful actors (e.g., governments). In order to make claims, actors, groups, or social movements rely on a set of a contentious repertoire that depends on the type of actor, political opportunity structures and temporal advancements (Tarrow and Tilly, 2007, p.49). For example, classical means within this repertoire of contention are rallies, demonstrations, sit-ins, petitions, but also more violent measures such as strikes, sabotages, and riots (Tilly, 2003). On an abstract level, an action repertoire is "the whole set of means [a group] has for making claims of a different kind on different individuals or groups" (Tilly, 1986, p.4). However, this does not imply that this set is static. Quite in the contrary, the literature emphasizes that action repertoires are open for innovation and advancements (Tarrow and Tilly, 2007).

The Internet has largely expanded the contentious action repertoire for social movements and groups. Van Laer and Van Aelst (2010) frame this extension as "[the] digitalized action repertoire" and distinguish between Internet supported and Internet-based action. On the one hand, the Internet supports groups and social movements in organizing classical means of action. The Internet reduced costs for collective action. For activists, it is easier to coordinate as well as communicate, both between group members and society at large (cf. Breuer, Landman and Farquhar, 2015; Diamond, 2010; Enikolopov, Makarin and Petrova, 2018; Little, 2016; Lupia and Sin, 2003; Tufekci and Wilson, 2012). Besides, information transmission became generally faster (Little, 2016). On the other hand, the Internet also created actions that are exclusively used online. For instance, as a new tool of contention it is possible to write online petitions, send email bombs or to use more disruptive actions such as DoS attacks, website defacement or other hacking actions (Van Laer and Van Aelst, 2010, p.1149). Finally, the Internet as a novel arena of contention did create not only new actions but also new Internet-based actors emerged (Martin, 2005). Examples of these actors are so-called "hacktivist" groups such as the group *Anonymous* or other globally active hacking groups (Coleman, 2014; Wong and Brown, 2013; Milan, 2015)

One of the most frequently used tools by these groups are DoS attacks. In contrast

to website defacements, website intrusions, and other forms of hacking, DoS attacks require relatively low technical skills and can be easily conducted (Dolata and Schrape, 2016; Milan, 2015; Olson, 2013). Thus, not only hacktivist groups use DoS attacks but also opposition groups may employ them as a new tool for contention. Most commonly, activists mount attacks jointly or use botnets or other amplification techniques to make their attacks stronger.[5] In fact, previous conceptual works state that mass participation is one requirement for a contentious DoS action (Jordan, 2002; Sauter, 2014).[6]

Concerning the timing of DoS attacks, anecdotal evidence and case studies highlight that activists use these attacks in response to real-world political events (Coleman, 2014; Olson, 2013; Sauter, 2014). For example, *Anonymous* and other activists mounted DoS attacks during the 2009 Iranian protests and 2011 Arab uprisings in order to protest against these authoritarian and repressive regimes and to gain media attention (Beyer, 2014; Coleman, 2014). More systematically, conducting a large-N analysis of English newspaper articles mentioning politically motivated DoS attacks, Asal et al. (2016) investigate which country-specific characteristics are associated with DoS attacks on a country-year level. The authors focus on the contentious use of DoS attacks by non-state actors, arguing that state repression leads to a higher probability of attacks. The study finds that human rights violations increase the likelihood of attacks. Additionally, the control variable number of protests appears to be the best predictor for the occurrence of DoS attacks. This finding suggests a complementary use of off- and online protest (cf. Holt et al., 2017).

In conclusion, the social movement literature agrees that DoS attacks are a new form of contentious action for hacktivists and activists (cf. Coleman, 2014; Wong and Brown, 2013; Sauter, 2014). However, concerning the use of DoS attacks as contentious tool there are still important questions unanswered. Although there is preliminary systematic work done on the occurrence of attacks (Asal et al., 2016), this work investigates this relationship at a highly aggregated level and is unable to explore dynamic effects. Besides, since the authors rely on newspaper articles to study DoS attacks, their study likely suffers from media biases, a problem, I will come back to in subsection 1.1.4.[7]

1.1.2 Previous Literature from an Authoritarian Politics Perspective

In this subsection, I briefly introduce the literature on authoritarian politics and how modern ICTs changed the tools governments have to stay in power. Then, I integrate the use of DoS attacks as a tool for authoritarian regimes to censor opposition voices and present anecdotal evidence for this use. Finally, this section again closes with a

[5] Botnets are connected devices that can be controlled by a so-called botnet master to start DoS attacks (or other actions). This can either happen voluntarily where users agree that their device is used for this purpose or non-voluntarily where the device is corrupted and "hijacked" through malware.

[6] Other requirements are direct action and virtual engagement (Jordan, 2002).

[7] Additionally, the study by Asal et al. (2016) lacks from some other empirical shortcomings, problems of endogeneity, for example.

discussion of the gaps in this branch of literature.

One of the main questions in the literature on authoritarian politics is how autocrats stay in power (e.g., Svolik, 2012). Comparable to the contentious repertoire groups and social movements have, authoritarian regimes can also rely on a toolkit of actions to achieve this goal. Generally, autocrats can use repressive means, co-optation, or both, to stay in power. Whereas co-optation describes the inclusion of certain groups into the elite circle of regimes, repression is more broadly used. Repression can be further distinguished into two types: Physical repression, including beatings, tortures etc., and censorship/information control of larger parts of the population (e.g., Frantz and Kendall-Taylor, 2014; Friedrich and Brzezinski, 1965; Wintrobe, 2000).

Modern ICTs, primarily the Internet, increased the number of censorship and repression tools for autocrats.[8] It appears that authoritarian regimes have learned how to reduce the "liberation potential" of the Internet (Diamond, 2010). This term refers to the advantages of the Internet with regard to information gathering, coordination, and communication, which were stated in the previous subsection. In fact, previous empirical literature fails to find evidence that increased Internet access lead to democratization (Rød and Weidmann, 2015). The possibilities to control the Internet are extensive for authoritarian governments, in particular. First, countries pass legal restrictions limiting the access to certain unwanted websites (Deibert and Rohozinski, 2010). Second, governments can also force Internet service providers to delete specific content as it is done in China, for example (King, Pan and Roberts, 2013). Third, many authoritarian regimes harass online bloggers and discredit them in social networks (Pearce and Kendzior, 2012; MacKinnon, 2013) or use the Internet and social media for their own propaganda employing trolls and other techniques (e.g., Gunitsky, 2015; MacKinnon, 2013; Tufekci, 2017; Munger et al., 2018). For instance, in recent articles Munger et al. (2018) and King, Pan and Roberts (2017) show that governments flood social media with content to distract users from sensitive issues. Finally, authoritarian regimes have also several technical possibilities to censor online, ranging from Internet Protocol (IP) filtering, Domain Name System (DNS) tampering to DoS attacks (Deibert et al., 2008).

Sophisticated regimes such as China and Saudi-Arabia, combine all different kinds of censorship possibilities and have even created a sort of closed "national network" (Boas, 2006; MacKinnon, 2013; King, Pan and Roberts, 2013; Roberts, 2018). Recently, former Soviet states have started to create similarly closed and controllable national networks (Gunitsky, 2015, p.50).[9] In addition to technical censorship solution, at least China also employs human-intensive methods of information control (the so-called "50 Cent Army") to censor and influence social media content (Roberts, 2018). A more drastic but less sophisticated tool of information control were the outages of the Egyptian and

[8] In fact, also co-optation efforts might be achieved more easily (e.g., Gunitsky, 2015).

[9] In contrast to China and Saudi-Arabia this is done post hoc, making it harder to control every already existing Internet nods.

Libyan Internet networks during the Arab uprising (Dainotti et al., 2014; Hassanpour, 2014) or shorter network outages during the civil conflict in Syria as a tactic to weaken the opposition (Gohdes, 2015). Yet, while there have been studies aiming to explain factors driving general Internet censorship (Hellmeier, 2016), specific tactics of censorship particularly in China (e.g., MacKinnon, 2013; King, Pan and Roberts, 2013; Roberts, 2018) and Internet outages (e.g., Hassanpour, 2014; Gohdes, 2015), there has been no systematic study of DoS attacks as another prominent, technically simple and relatively low-cost censorship tool open to a wide range of semi-democratic and authoritarian regimes.

Anecdotal evidence highlights that pro-regime groups or government-related hackers often conduct DoS attacks and that these groups are likely "hired" by authoritarian governments (Deibert and Rohozinski, 2010, p.53). For example, in a report by Marczak et al. (2015), the authors illustrate how perpetrators used DoS attacks in 2015 to attack two websites, GreatFire.org and Github.com, which offer tools to circumvent Chinese censorship. In their analysis, the authors show how malicious Chinese servers, likely infected by Chinese authorities, attacked the websites mentioned above. Another report illustrates how attackers used DoS attacks against independent and opposition media websites in Azerbaijan. In this case, the researchers could trace some of the attacks back to government-owned IP ranges (Qurium, 2017).

Nevertheless, in most cases, it is difficult to pinpoint the perpetrator of DoS attacks, and only the target can be analyzed. For example, before the Russian election in late 2007, the website of the opposition politician and chess player Gary Kasparov was targeted by massive DoS attacks (Nazario, 2009, p.6). Other examples are DoS attacks on online radio and TV stations, as well as newspaper websites, during the Russian 2011 elections and protest afterward (Jagannathan, 2012; Shakarian, Shakarian and Ruef, 2013). Anecdotal evidence suggests that the Russian government "ordered" many of these attacks and that government-related groups conducted them, e.g., the pro-Kremlin group *Nashi* using botnets (Carr, 2011). Beyond Russia, there are reports of DoS attacks on Burmese opposition websites, especially when there were important events such as protest anniversaries or upcoming elections (Villeneuve and Crete-Nishihata, 2012) or attacks on media outlets in Ecuador that reported on protest events in 2015 (Freedom House, 2016). Overall, these examples highlight that opposition and independent news websites appear to be often targeted during contentious periods and that government or government-related actors are likely behind these attacks. In a similar vein, Zuckerman et al. (2010) emphasize that DoS attacks are increasingly used to silence human right and independent media websites. The researchers surveyed human rights and independent news agencies in a set of authoritarian countries, highlighting that above 62% of the respondents experienced DoS attacks.[10]

[10]This number might be overestimated as organizations that were targeted more likely responded to the survey for which the response rate was only 14% of 317 organizations asked (Zuckerman et al., 2010,

Overall, there is a reason to believe that DoS attacks are a convenient tool to censor and silence critical voices in authoritarian countries. Nevertheless, thus far, there has been no theoretical work on the question of why, when, and for what exact censorship purposes authoritarian governments use DoS attacks. Furthermore, the literature is missing systematic work on the use of DoS attacks in this context. It is these gaps I am filling in my dissertation.

1.1.3 Previous Literature from an International Relations Perspective

Finally, in this subsection, I summarize the literature on the use of cyberattacks for interstate conflict and discuss the use of DoS attacks in this context. Subsequently, I again highlight the shortcomings of this body of literature.

Most of the research on cyber conflicts is situated in the field of security studies and focuses on individual cases only. While some of these studies claim that the world is at the verge of a cyberwar (e.g., Richard, Robert et al., 2010; Lynn III, 2010), other authors state that cyber tactics play only a limited role in overall military and foreign policy strategies (e.g., Rid, 2012; Gartzke, 2013). A first reason for the latter is that cyberattacks have not led to casualties, at least for the moment (Gartzke, 2013). A second one is that they are on average not as effective and only temporary (Gartzke, 2013; Valeriano, Jensen and Maness, 2018). Besides, deterrence of cyberattacks remains challenging as it is often not possible to determine the exact attacker of cyberattacks and attribution and retaliation therefore remains difficult (Nye Jr, 2017; Deibert, Rohozinski and Crete-Nishihata, 2012; Rid and Buchanan, 2015; Poznansky and Perkoski, 2018). These factors are, in particular, valid for low-cost cyber attacks. In contrast, so-called Advanced Persistent Threats (APTs), custom-tailored high-skilled cyber actions, can often be attributed to specific states (Geers et al., 2014).

More systematically, in various articles and books, Valeriano, Maness, and Jensen classify cyberattacks into, potentially coercive, policy tools: disruption, espionage, and degradation. Digital disruption tactics include DoS and defacement campaigns, espionage the use of hacking and network intrusion, and degradation describes large-scale cyber operations, e.g., the Stuxnet malware against the Iranian nuclear program in 2010 (e.g., Valeriano, Jensen and Maness, 2018). In one of the first empirical studies on the topic, Valeriano and Maness (2014) show that cyberattacks are not as frequently launched analyzing media-based data on cyber incidents between rival states from 2001–11. Nevertheless, they identify DoS attacks as the most commonly used tool for interstate warfare. Further empirical studies in this field have primarily focused on the question of the impact of cyberattacks, e.g., on worsening interstate relations and concessions (Maness and Valeriano, 2016; Valeriano, Jensen and Maness, 2018). Here, the authors find only limited evidence for an impact of cyberattacks on both outcomes.[11]

pp.33-34)

[11] Although the authors find that DoS attacks lead to worsening interstate relations, this result remains

One main shortcoming of these empirical studies is their exclusive use of publicly available data (i.e., media reports) to capture DoS and other cyberattacks. By this, these studies may portray a biased picture of the use of cyberattacks as many incidents are likely not reported publicly and only significant and successful attacks captured (Poznansky and Perkoski, 2018). An exception is a recent scholarly work by Kostyuk and Zhukov (2019) that investigate the interplay between DoS attacks and battlefield events in Ukraine and Syria using data of DoS attacks by an Internet security company. Their empirical results show no relationship between cyber and actual battlefield events. A potential explanation for this null finding might be that cyberattacks are not coordinated by the Russian or Syrian authorities, respectively. Supporting this explanation, Deibert, Rohozinski and Crete-Nishihata (2012) argue in a case study on the 2008 Russo-Georgian war that not necessarily state actors were responsible for DoS attacks in this case but private citizens and patriotic hacking groups that launch them to support their country. In a similar vein, Rid (2012) states that the large-scale DoS attacks against in Estonia 2007 were likely started by patriotic Russian citizens and groups and not necessarily coordinated by the Russian government.

In conclusion, we know little about the motivation and timing of DoS attacks during interstate conflict. Furthermore, previous studies have been limited by the unavailability of comprehensive data on cyber incidents.[12] Additionally, the studies by Valeriano and Maness assume that governmental actors are necessarily behind these attacks. For DoS attacks this assumption may not always be accurate as due to their simplicity patriotic or private groups may be responsible for DoS attacks during international disputes as well (cf. Deibert, Rohozinski and Crete-Nishihata, 2012).

1.1.4 Gaps of the Previous Literature

Before I introduce the main contributions of my dissertation in the next section, I summarize the identified three main gaps from the literature review: disconnected literature, missing empirical studies and media biases of previous works.

Disconnected literature The review revealed that the literatures concerned with the political use of DoS attacks are disconnected. The international relations literature concerning cyberattacks and conflict largely neglect the possibility that DoS attacks may be also launched by activists and non-state groups. Besides, it may be also domestic reasons that trigger DoS attacks. The studies from the social movement literature only focus on non-state groups and activists as likely perpetrators. In contrast, the potential censoring use of DoS attacks by authoritarian governments or their proxies has received the least academic attention so far. For this branch of literature, it remains unclear when and for what purposes authoritarian governments use these attacks. In conclusion,

correlational.

[12] A point that is also put forward by Valeriano, Jensen and Maness (2018, p.209) themselves.

the literature lacks from a unified theoretical framework on the use of DoS attacks in authoritarian regimes.

Missing empirical studies Most of the studies from the different fields of study are either anecdotal accounts or case studies only. Although there is previous empirical work done, in particular when it comes to the use of DoS and cyberattacks in international conflict, systematic work from the other fields of study is rare. This is again especially true for the use of DoS attacks as a potential censorship tool for authoritarian governments. Regarding the few empirical studies from the international relation and social movement literature, these can only partly answer why and when actors use DoS attacks for political purposes. First, the empirical analyses of these studies are aggregated to a year- or cyber campaign level, making the investigation of dynamic relationships and inference challenging. Second, most of the cyber conflict studies are concerned with the impact of these attacks but do not investigate the reasons for their use. Although systematic studies on the impact of DoS attacks for the other fields of study are also missing, an investigation of consequences makes only sense when it is known how widely DoS attacks are used for what purposes. Therefore, the main goal of this dissertation is to explain the differentiated political uses of DoS attacks and show how frequently political actors use them in autocracies. In the dissertation's conclusion, I will return to the question of the political effects of DoS attacks and discuss whether future research should move forward in this direction.

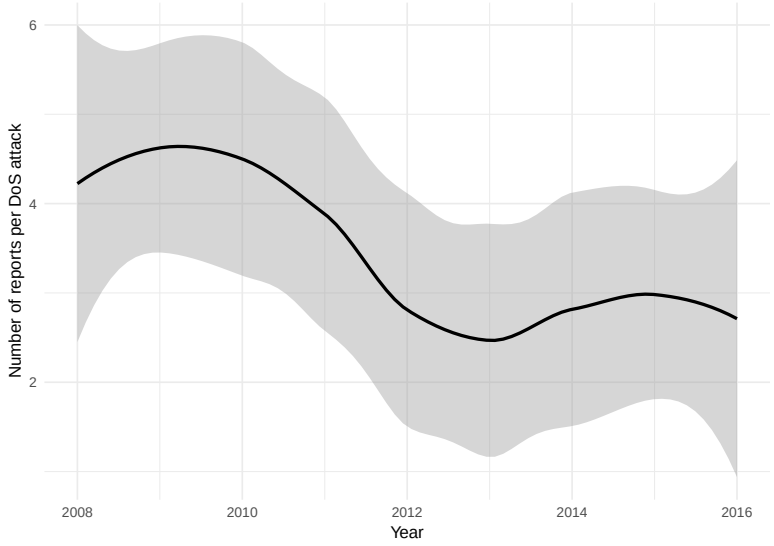

Figure 1.2: Average number of article reporting on DoS attacks 2008 - 2016. Note: The media-based data collect news reports mentioning politically motivated DoS attacks. This allows to calculate the average number of reports per DoS event. 95% confidence intervals are displayed.

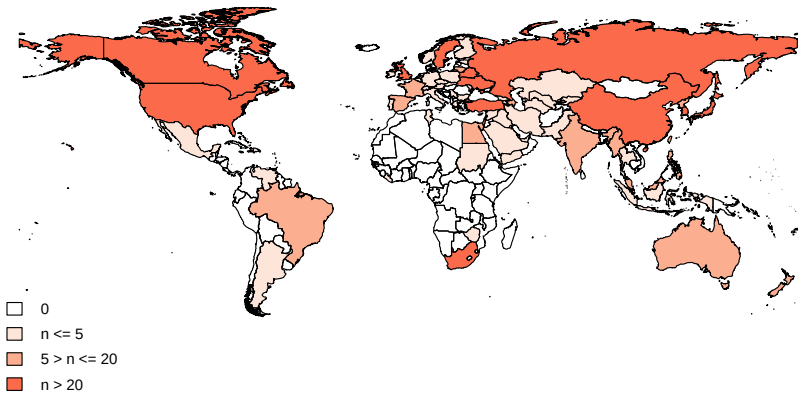

Figure 1.3: Number of politically motivated DoS attacks from English-language newspapers 2008 - 2016. Country borders based on Weidmann, Kuse and Gleditsch (2010).

Media biases of previous work For the few systematic studies exploring DoS attacks from an international relations or social movement angle, there may be one serious source of bias. Most of these studies rely on newspaper articles to code politically motivated DoS attacks and may therefore suffer from media biases.[13] First, newspapers can only report on publicly known DoS attacks. Since most cyberattacks are covert and/or unsuccessful, previous studies likely missed a large share of attacks as well as attempts thereof (cf. Poznansky and Perkoski, 2018). In particular, according to previous work, news agencies often do not report DoS attacks against opposition, human rights, and newspapers in authoritarian countries (Hardy et al., 2014). Second, as newspapers are driven by the newsworthiness of events, they might only report on spectacular and bigger attacks (cf. Earl et al., 2004). Besides, the interest in DoS attacks may also decrease over time. While in 2009, the use of DoS attacks was a relatively new phenomenon, today, DoS attacks might not attract a reader's attention. News outlets therefore may decide to not report about them at all. Figure 1.2 supports the previous point and highlights that the number of reports per DoS events, which is perceived as an indicator for interest, decreased over the years. Third, by using media-derived data the challenge is that factors of interest that may explain DoS attacks (e.g., election periods) might not be only related to an increase in actual DoS attacks, but also to the reporting thereof because the country is in the center of attention, for example. With this measurement error, inferential statistics may lead to biased results (cf. King, Keohane and Verba, 1994). Finally, previous research mainly relied on English newspapers and reports (cf. Asal et al., 2016; Valeriano and Maness, 2014). My own media-based data, which also relies

[13] An exception is the study by Kostyuk and Zhukov (2019).

on English sources, highlights that this leads to a clear bias towards English-speaking and geopolitically important countries. Figure 1.3 shows that the data record only very few politically motivated DoS attacks in the Americas and Africa, while a large number of attacks in the USA, Great Britain, China, and Russia.

1.2 Contributions

In the next subsections, I discuss how I aim to address the identified gaps in my dissertation, before I introduce my three papers in the next section.

1.2.1 Towards a Unified Theoretical Framework

The first goal of this dissertation is to connect the three bodies of literature and to explain the differentiated use and the occurrence of politically motivated DoS attacks in authoritarian regimes. I argue that the main political uses of DoS attacks in this context are to censor and contend. The former describes DoS attacks as a convenient tool for authoritarian governments and government-related groups to censor online, whereas the latter aims at the use of DoS attacks as a tool by domestic and international activists *or* governments or pro-government groups to disturb servers as a sign of protest.[14] In the first paper (Chapter 2), we argue that both motivations may explain an increase of DoS attacks during election periods in autocracies because governments have incentives to censor threatening websites, and activists to protest electoral frauds or repressive government policies. In the second paper (Chapter 3), I explore the censorship mechanism in more detail by focusing on DoS attacks on online news outlets in Venezuela. Here, I propose that DoS attacks may not only be used to censor information temporally but also to send repressive signals to the news outlets. Finally, in the third paper (Chapter 4), I propose that the contend mechanism of DoS attacks may also apply to authoritarian governments or pro-government groups launching DoS attacks against other states when these target their own country with aggressive foreign policies.

1.2.2 Towards a Systematic Empirical Analysis

Overall, empirical studies of the political use of DoS attacks remain limited. The second goal of this dissertation is to fill this gap by systematically studying the use of DoS attacks in autocracies on a temporally disaggregated macro and micro level. Besides, instead of using the collected media-based data to capture DoS attacks, I rely on two different data sources and measurement approaches that are independent of media reports.

[14] To be clear, these are not exclusive mechanisms, yet the primary motivation to launch DoS attacks is different.

Passively measured data The primary dataset comes from a collaboration with the Center of Advanced Internet Data Analysis (CAIDA) at the University of California, San Diego. Their data capture so-called "randomly spoofed" DoS attacks worldwide from 2008 until today with a high spatial and temporal resolution (CAIDA, 2016; Jonker et al., 2017). "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. By this, attackers hide their true identities and make it also more difficult for a victim to fend off an attack by simply blocking incoming traffic from a particular address (Zargar, Joshi and Tipper, 2013). CAIDA can measure these attacks by monitoring a large address space of unassigned IPv4 addresses. This passive measurement works because attacked servers still respond to the "fake" IP address of the attacker. This response eventually falls within the IPv4 address range monitored by CAIDA enabling to passively measure DoS attacks (see Moore et al., 2006, for more details). Apart from taking care of media biases, the data come with two additional advantages. First, the measurement is worldwide comparable and highly temporally disaggregated, allowing to conduct time-series cross-country analyses.[15] Second, the data even include DoS attack attempts, making an investigation of the use of DoS attacks less biased.

Nevertheless, some limitations remain. First, I am only able to use this data aggregated on the country level, allowing to investigate macro developments only. Second, the data rest on three underlying assumptions of how DoS attacks are generated. The spoofing process has to be (uniform) randomly, the packets have to be reliably delivered to the victim and CAIDA, and captured packets could also reflect purely network scanning activities (Moore et al., 2006). While Moore et al. (2006) show that most of their captured traffic is different from scanning activities, they admit that the first and second requirements might underestimate the overall level of DoS attacks. In the first and third paper, I will discuss the advantages and limitations of this data source again in greater detail.

Actively measured data In order to investigate micro dynamics, I use a second measurement approach, where I aim to capture DoS attacks by monitoring online statuses of news websites continuously. These countries include all authoritarian countries that hold elections in 2018.[16] For the measurement, I set up a server that sends status code requests to news websites in these countries and saves the websites' response codes. To infer DoS attacks, I exploit the so-called Hypertext Transfer Protocol (HTTP) of how web servers communicate, where servers return standardized codes to web server

[15] Data from computer security companies may be biased in that regard as their technologies are differently employed worldwide.

[16] Including news websites from Azerbaijan, Congo, Cameroon, Cuba, Egypt, Iraq, Mali, Malaysia, Mauritania, Russia, Rwanda, South Sudan, Thailand, Swaziland, Turkmenistan, Venezuela, and Zimbabwe.

requests telling if they are reachable or not. While this approach has the advantage that I measure potential DoS attacks on a fine-grained website resolution, this approach is only able to capture successful DoS attacks, the ones that lead to an outage of a website, and the chances of false-positives may be higher. In the second paper, I discuss the advantages and limitations of this data source in greater detail.

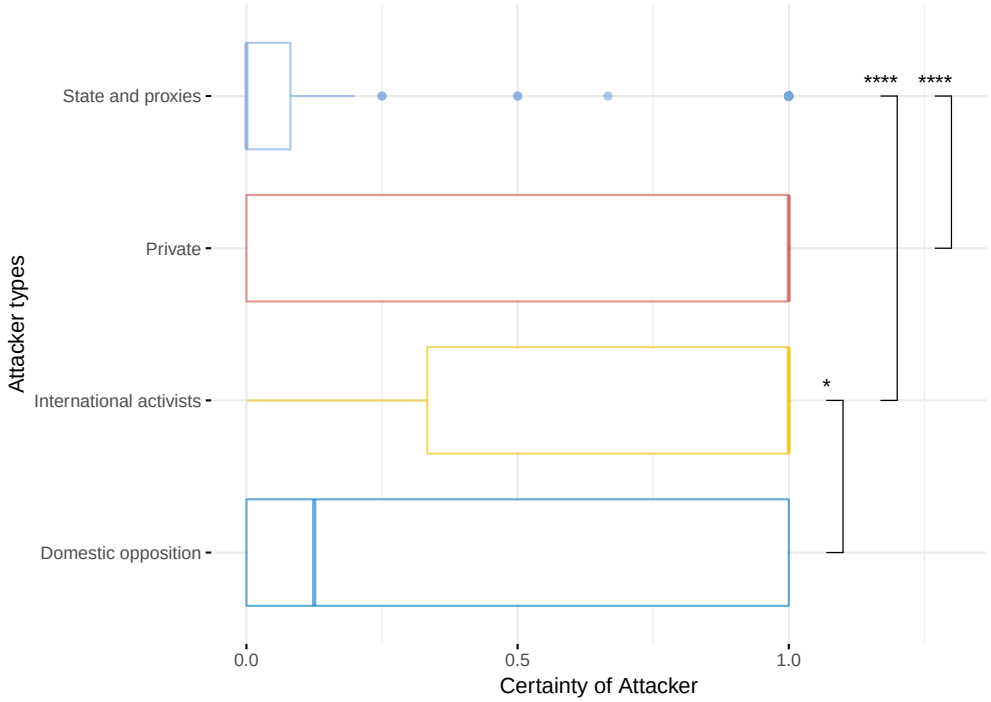

Figure 1.4: Certainty of Attacker in DoS attacks. Note: The level of certainty ranges from 0 (not certain) to 1 (certain) and is only available for DoS events where news articles mention potential perpetrators. If more than one article mentions a perpetrator, I calculate the average value (see Appendix B for more details). Only t-tests for significant comparisons are shown. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

Attribution problem One hard-to-solve problem in studying cyberattacks is that these attacks are often not traceable. This means that researchers can only rely on information about the victim of the attack but not on the perpetrator. This so-called attribution problem also remains true for the taken empirical approaches in my dissertation. While it could be argued that using media-derived data can circumvent this problem, Figure 1.1 shows that it is frequently unknown who is behind a DoS attack. Besides, even if newspapers suspect an attacker this remains mostly uncertain (cf. Villeneuve and Crete-Nishihata, 2012). Indeed, Figure 1.4 illustrates that in particular for DoS attacks by supposedly government or government-related actors, the certainty of newspapers with regard to their attribution goes to zero. In contrast, the figure shows that international activists and private actors often claim responsibility for the attack to gain attention and rewards (cf. Poznansky and Perkoski, 2018). Nevertheless, they

can do so only for successful attacks.

Generally, the attribution problem of cyberattacks is hard to solve in systematic empirical studies as it is in the nature of these attacks that they are difficult to trace back. Thus, while my empirical approach is not able to determine the exact perpetrators and can only focus on the victims of DoS attacks, I employ theoretical reasoning and rely on anecdotal evidence in the three different papers to pinpoint the actors that have the highest motivation to attack the respective targets in the different settings.[17]

1.3 Dissertation Synopsis

In the following, I briefly summarize the arguments, findings, and implications of each paper.

1.3.1 Paper 1 – At Home and Abroad: The Use of Denial-of-Service Attacks during Elections in Non-democratic Regimes

In the first paper (Chapter 2), which was written together with Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti, the main goal is to study whether the examples of the politically motivated DoS attacks against opposition and news outlets as well as government websites are systematic in autocracies. To explore this, we investigate whether the frequency of DoS attacks increases during election periods as one of the political focal points in countries worldwide.

In the paper, we argue that an increase in DoS attacks during election periods should be especially pronounced in authoritarian countries. One the one hand, governments in power have high incentives to use these attacks against unwanted news, opposition, and other threatening websites (censorship mechanism). On the other hand, activists may use DoS attacks more likely to protest against electoral fraud and/or increased repression (contention mechanism).

In the empirical part, we make use of the DoS data mentioned above provided by CAIDA. We look at the development of DoS attacks from April 2008 until December 2016 on a one-week granularity and combine this data with information on elections. By using this data source, our analysis is not prone to media biases, and we can study the development of DoS attacks globally. We then run statistical models that compare the number of DoS attacks during election periods with the average number of DoS attacks per country and year. Furthermore, our study does not only investigate the development of DoS attacks on the countries, but we also measure DoS attacks on states where the respective country hosts its news websites. With this, we are better able to investigate

[17] A potential solution could be to collect data from perpetrators of attacks. However, while it may be possible to join Internet Retail Chats (IRC) of groups such as *Anonymous* (cf. Olson, 2013) to collect calls for DoS attacks, this is undoubtedly more difficult, if not impossible, for government-related hacking groups or authoritarian government entities.

potential attacks on news and likely other critical websites because they are frequently not hosted in the country of origin, especially if the regime is authoritarian.

The results display a higher number of DoS attacks during election periods in more authoritarian countries. However, contrary to our expectations, this increase is not as robust and profound for DoS attacks on the country. Instead, we observe an apparent increase of DoS attacks against countries where autocracies host their news websites. This finding lends support to the censorship mechanism of DoS attacks, where authoritarian regimes appear to export censorship abroad by attacking websites hosted in other countries. From a policy perspective, this result emphasizes the importance of protecting independent websites during contentious times to ensure that domestic and international audiences can still access regime critical and independent information.

1.3.2 Paper 2 – Hot Topics: Denial-of-Service Attacks on News Websites in Autocracies

The Internet offered news outlets a new way to evade press censorship in authoritarian government. However, authoritarian governments have learned how to censor in the online sphere as well. While the first paper finds macro-level evidence for the systematic use of DoS attacks as one understudied tool to censor online, questions related to when, why and what websites are targeted could not be sufficiently answered. To answer these questions, the second paper (Chapter 3) focuses on the micro-level and explores the reasons for DoS attacks against news websites in autocracies.

The study focuses on the case of Venezuela and monitors the online status of 19 news websites from November 2017 until June 2018. I argue that the use of DoS attacks against news websites can follow two censorship mechanisms. First, governments or government-related actors use these attacks to temporarily disable the complete website when sensitive content is published ("just-in-time censorship"). And/or second, attackers launch DoS attacks as a repressive response to punish outlets for their reporting ("repressive censorship"). The goal of the first mechanism is that citizens do not see sensitive information, while the second mechanism can be understood as a repressive and economically costly signal to the respective media outlets that the actual and previous reporting was unwanted.

In the empirical part, I monitor the status of several non-state news websites in Venezuela and retrieve a website's status code, allowing to infer potential DoS attacks. To investigate whether news content matters, I retrieve the websites' front-page headlines every day. Then, I employ topic models for short-text and aggregate news websites headlines to broader topics. Finally, I run statistical models that control for newspaper- and time-specific factors that may influence the content of a newspaper and whether the website gets attacked. To further distinguish between my two theoretical mechanisms, one model looks at the reporting of news on the same day, while another model

at the aggregated reporting of news up to one week before. Whereas, by definition, the just-in-time censorship mechanism can only apply in the short-term, repressive DoS attacks may be triggered by content in the short- and medium-term. Thus, positively related sensitive topics in the medium-term and short- *and* medium-term would support the repressive use of DoS attacks. In contrast, topics that are exclusively positively related to the likelihood of DoS attacks in the short-term, rather support the just-in-time censorship mechanism.

The results show that only a few sensitive topics clearly increase the likelihood of DoS attacks on news websites on the same day. In contrast, topics on general socio-economic questions, sanctions, Maduro and some international topics, lead to a higher likelihood of DoS attacks in the medium term. While these results lend support to both mechanisms, the more pronounced use of DoS attacks appears to be the punishment of news outlets for reporting on sensitive topics. The study advances our understanding of both offline and online censorship and shows that the goal of DoS attacks is not only to restrict information temporally but even more to spread fear.

1.3.3 Paper 3 – Digital Responses to Sanctions? Denial-of-Service Attacks against Sender Countries

The third paper (Chapter 4) focuses on the international dimension of DoS attacks and ask how widely they are used for interstate conflicts. Whereas many pundits and one strand of the cyber conflict literature argue that cyberattacks are a new coercive policy tool in international relations (e.g., Richard, Robert et al., 2010), theoretical works disagree and state that these attacks are ineffective for coercion (e.g., Rid, 2012; Gartzke, 2013). The goal of this paper is to test these claims empirically. More precisely, I investigate one likely case where one should expect the use of DoS attacks as a response to aggressive foreign policy: the threat or imposition of sanctions by the United States and European Union.[18]

I propose two mechanisms for why this could be the case. The first follows one branch of the literature and suggests that the targeted state uses DoS attacks as a coercive mean to create disruption costs and send a resolve signal to the sender state(s) that should help to gain concessions (prevent sanctions or lift them). The second offers an alternative mechanism, where governments and/or actors within the target state use DoS attacks as a digital response to protest against the aggressive foreign policy. Furthermore, the second mechanism should be more applicable in the case of the imposition of sanctions as patriotic sentiments are reinforced more strongly, and elites and citizens are affected

[18]Since the main argument in this dissertation is that authoritarian governments or individuals/groups within these countries use DoS attacks primarily for domestic purposes, the investigation of liberal sanctions as an international cause enables me to see whether this is true. In fact, as around 85% of sanctions by the United States target non-democratic countries (Kaempfer, Lowenberg and Mertens, 2004), the focus on sanctions allows me to have a valid comparison.

by the sanctions. Instead, the first mechanism makes rationally more sense already after sanction threats to avoid economic costs at all and more easily achieve concessions.

For the empirical analysis, I again rely on the data provided by CAIDA. This time, I use daily time series for DoS attacks on the United States and European Union as the most active sanctioning entities. Then, I run time series models and use simulation approaches to determine how sanction threats and impositions influence the development of DoS attacks on the US and EU. The results highlight no statistically significant relationship between sanction threats and DoS attacks. With regard to sanction impositions, only sanctions targeted on countries with a certain level of technological capabilities appear to increase the level of DoS attacks on the United States. While this points to some systematic pattern, further robustness and sensitivity tests highlight that this result is largely driven by a few cases only.

In conclusion, there seems to be no systematic relationship between sanctions and the development of DoS attacks in sender countries. Furthermore, as supported by an in-depth analysis of the development of DoS attacks on Russia in 2014, the results suggest that more likely patriotic hacking groups and citizens are behind an increase of DoS attacks and that DoS attacks do not necessarily follow a rational state logic. These findings question the use of DoS attacks as a coercive instrument in international relations. Instead, it appears that in this context DoS attacks are, if at all, employed as a contentious response to show disapproval.

2

At Home and Abroad: The Use of Denial-of-Service Attacks during Elections in Non-democratic Regimes

Co-authored with Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti
Journal of Conflict Resolution, 64(2-3):373–401, 2020
DOI: 10.1177/0022002719861676

Abstract: In this article, we study the political use of Denial-of-Service (DoS) attacks, a particular form of cyberattack that disable web services by flooding them with high levels of data traffic. We argue that websites in non-democratic 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.

2.1 Introduction

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 inter-state 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 paper 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 non-democratic regimes (Freedom House, 2017*b*). 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 dataset 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 non-governmental groups (Hardy et al., 2014, p.1). This attack dataset 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 dataset, 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.

2.2 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 government-related 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.

2.2.1 A Tool for Censorship

According to Freedom House (2016), more than 35% 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 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 shut down 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 also 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 Internet Service Providers (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 non-democratic 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 country-wide firewalls,

[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).

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 suggests that DoS attacks are not only attractive for clearly non-democratic regimes but already 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 government-related 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 it's 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 patriotic 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).

2.2.2 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 pow-

erful and visible tool to show disagreement. If, for example, government websites, mail servers or official news agency of a country are 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, pp. 551f). Nevertheless, some basic understanding of Internet technology is necessary for this. For example, many activists that 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 above mentioned 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 anti-regime protests against authoritarian regimes in the 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, pp. 152f). 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.

2.2.3 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) as well as gain legitimacy (Schedler, 2013). At the same time, elections constitute some of the most important focal points for anti-regime activities and political unrest within non-democratic 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 the Turkey in 2015, Russia in 2007, or Malaysia in 2011 (Freedom House, 2017*b*; 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 2.1 *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 2.2 *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 2.3 *The increase in (domestic and foreign) DoS attacks becomes stronger the closer the respective country is to an election.*

2.3 New Data to Measure Denial-of-Service 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 (for example, 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 non-democratic ones, are unlikely to be covered comprehensively. Lastly, Hardy et al. (2014, p. 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 government-related groups.

To remedy this issue, we rely on high-resolution attack estimates provided by the Center of Applied Data Analysis (CAIDA) at the University of California, San Diego

[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.

from 2008 to 2016 (CAIDA, 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 (approx. 1/256th of of all IPv4 Internet addresses). For more details on this estimation method, please refer to Moore et al. (2006).

Overall, our data record more than twenty-two million attacks during this period. Figure 2.1 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 2.2 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.

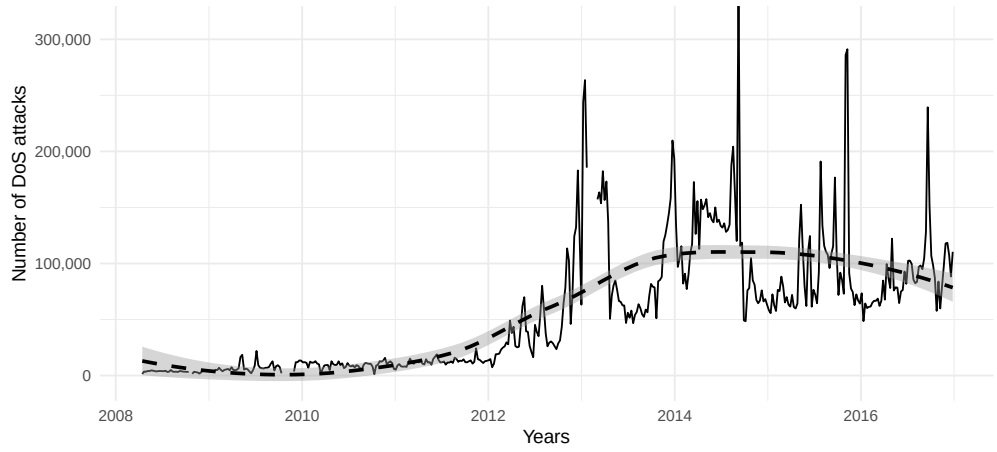

Figure 2.1: Number of DoS attacks 2008 to 2016 over time (in countries with elections). The dashed line shows the smoothed trend.

There are some significant advantages of our approach, since our data does 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 includes 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

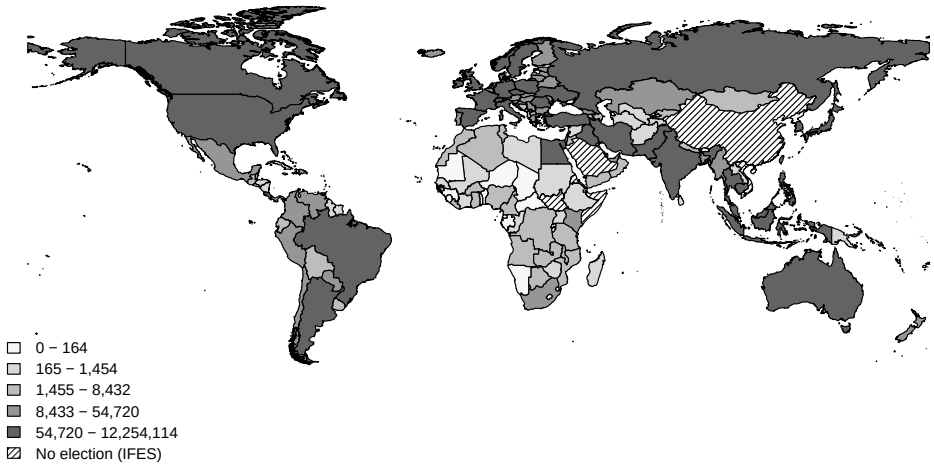

Figure 2.2: Number of DoS attacks 2008 to 2016 in countries with elections. Country borders based on Weidmann, Kuse and Gleditsch (2010).

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, p.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 its country of origin. Our analysis therefore focuses exclusively on the country of the target website.

2.4 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 1-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 (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

[4]We restricted the analysis to countries that are contained in the *Correlates of War* list of independent states (Singer, 1988).

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 C.1 in the Appendix.

Dependent variables To construct our dependent variables, we use CAIDA's dataset 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 (non-political vs. political, the latter against state- as well as non-state actors). Since we cannot distinguish between political and non-political 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, USA, UK, Germany, India, Australia), the dataset distinguishes between national and regional sites, and we only use the former. From the news website dataset, 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:

$$DoS\_foreign\_hosts_{it} = \sum_{j=1}^{N-i} p_{ij} * DoS_{jt} \tag{2.1}$$

where $N-i$ denotes all countries except country i, $p_{i,j}$ 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

[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 geo-location of servers, we additionally conduct robustness tests with a recalculated indicator, leaving out newspapers using this service (see Section 5.4).

attacks, in this case, on foreign hosts. Thus we can still not distinguish between political and non-political 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 2014–2016. 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 if 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, etc. 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) indicates that some of them are politically motivated, assuming that the level of non-politically motivated attacks does no 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:

$$ln(DoS_{i,t} + 1) = \beta_1 election_{i,t} + \beta_2 (election_{i,t} \times autocracy_{i,t}) + \delta_{i,t} + \epsilon_{i,t}. \quad (2.2)$$

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]

2.5 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.

2.5.1 Descriptive Evidence

Figure 2.3 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 anti-regime protests. Anecdotal evidence emphasizes that mainly activists were responsible for the attacks, targeting government websites in order to protest against election fraud and to support anti-regime 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*b*). 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 2.3 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

[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.

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.

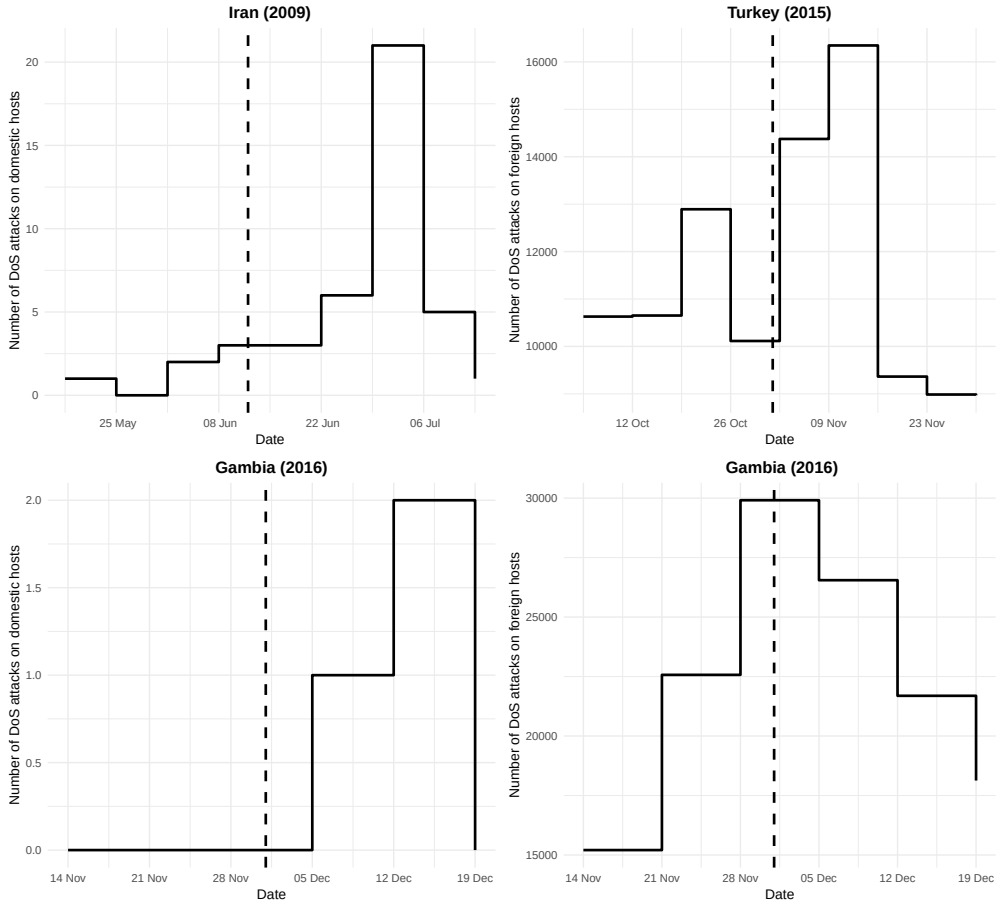

Figure 2.3: DoS attacks during election periods in Iran (2009), Turkey (2015), and Gambia (2016). The dashed black vertical line represents the election date, whereas the solid line illustrates the development of DoS attacks in the respective weeks.

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 non-election 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 $>= 0.5$).[7] Table 2.1 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

[7]We follow Lührmann, Tannenberg and Lindberg (2018) here, who use the same threshold to distinguish between autocracy and democracy.

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 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.

	Attacks on domestic hosts (2008-16)		Attacks on foreign hosts (2014-16)	
	Democracy	Autocracy	Democracy	Autocracy
Elections	557.99	106.32	18788.51	22304.41
No Elections	502.28	96.63	21699.88	21527.86

Table 2.1: Average number of DoS attacks per week on the country and on foreign hosts.

2.5.2 Main Models

Our main statistical models are reported in Table 2.2. The Models 1-2 use the logged number of attacks on the country, and Models 3-4 use the logged number of attacks on foreign hosts. Models 1 and 3 only include the (non-interacted) 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.

	Model 1 Domestic	Model 2 Domestic	Model 3 Foreign	Model 4 Foreign
Election period	-0.032^{*}	-0.039	-0.020	-0.096^{***}
	(0.014)	(0.030)	(0.012)	(0.026)
Election period × autocracy index		0.036		0.230^{***}
		(0.065)		(0.055)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81305	70817	28175	24503

Table 2.2: Relationship between election periods, level of autocracy and DoS attacks (country/week). Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

To better illustrate the estimated relationships of the interaction models, Figure 2.4 shows the estimated coefficient for elections periods conditional on the autocracy index. As already stated above, the models do not include the the main effect for the autocracy index as this variable is not varying on the year level and hence captured by

the country × year fixed effects. The left panel highlights the systematic relationship between the relationship of 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 2.1 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 are not systematically attacked during election periods in more authoritarian countries.

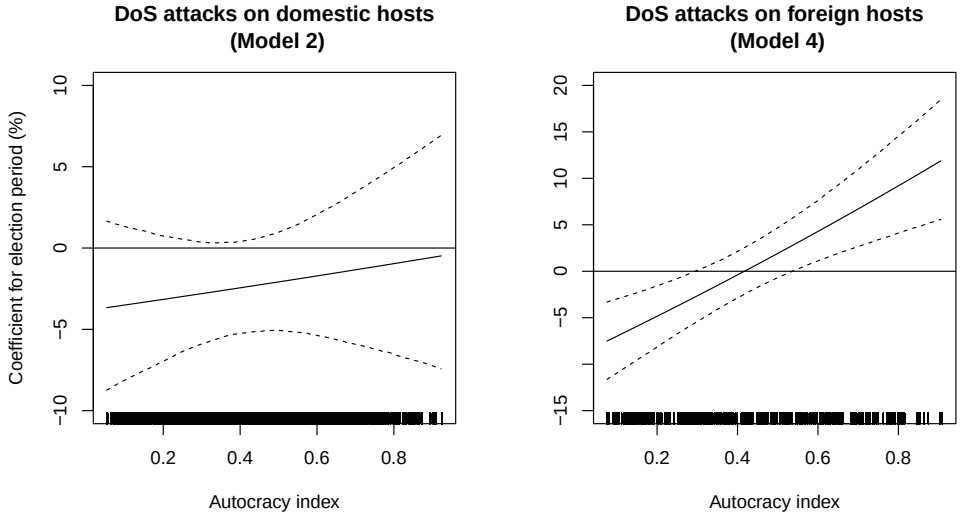

Figure 2.4: Effect of election period on DoS attacks, dependent on the level of autocracy. 95% confidence interval displayed with robust standard errors clustered at the country-year level. Simulations based on 10,000 draws. Observations towards the right of the panels correspond to more autocratic systems.

In contrast, in the right panel we observe a clearly positive trend when it comes to attacks on foreign hosts (see Hypothesis 2.2). The relationship between election periods and DoS attacks is the stronger the more authoritarian a country is. DoS attacks on foreign hosts increase by almost 15% 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.

2.5.3 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 2.3 shows that in the foreign host models, the coefficients of the 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 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 2.3 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) post-election period (each lasting three weeks), excluding the election week as here attacks could be captured before, during and after the election. Table 2.4 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 post-election 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.

2.5.4 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 non-democratic countries using the cut-off value of 0.5. Table C.3 shows the same patterns as in our main models. The table highlights that election

[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 in the Appendix also 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 non-interacted foreign host model as well. In contrast, the coefficient for temporal proximity alone in the domestic hosts model is not positive anymore.

(i) Election week (+ 2 weeks before and after)

	Model 5 Domestic	Model 6 Domestic	Model 7 Foreign	Model 8 Foreign
Election period	-0.034^{*}	-0.033	-0.027^{*}	-0.110^{***}
	(0.014)	(0.034)	(0.013)	(0.030)
Election period × autocracy index		0.021		0.244^{***}
		(0.074)		(0.063)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81477	70965	28345	24649

(ii) Election week (+ 1 week before and after)

	Model 9 Domestic	Model 10 Domestic	Model 11 Foreign	Model 12 Foreign
Election period	-0.020^{*}	-0.028	-0.029	-0.120^{**}
	(0.014)	(0.044)	(0.017)	(0.037)
Election period × autocracy index		0.042		0.264^{***}
		(0.097)		(0.080)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81655	71119	28521	24801

(iii) Only election week

	Model 13 Domestic	Model 14 Domestic	Model 15 Foreign	Model 16 Foreign
Election week	0.020^{*}	0.001	-0.040	-0.175^{**}
	(0.014)	(0.072)	(0.028)	(0.061)
Election week × autocracy index		0.072		0.370^{**}
		(0.164)		(0.138)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81840	71280	28704	24960

Table 2.3: Relationship between election periods, level of autocracy and DoS attacks (country/week). Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

(iv) Pre-election period

	Model 17 Domestic	Model 18 Domestic	Model 19 Foreign	Model 20 Foreign
Pre-election period	−0.037	−0.018	−0.034*	−0.048
	(0.019)	(0.043)	(0.017)	(0.038)
Pre-election period × autocracy index		−0.021		0.062
		(0.093)		(0.078)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81283	70795	28153	24481

(v) Post-election period

	Model 21 Domestic	Model 22 Domestic	Model 23 Foreign	Model 24 Foreign
Post-election period	−0.036	−0.064	−0.019	−0.136***
	(0.019)	(0.041)	(0.016)	(0.035)
Post-election period × autocracy index		0.076		0.334***
		(0.087)		(0.075)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81840	71280	28704	24960

Table 2.4: Relationship between pre- and postelection periods, level of autocracy and DoS attacks (country/week). Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

periods in non-democratic regimes are on average associated with an increase by 7.91% (3.99%; 11.84% [95% confidence intervals]) 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 Geo-referenced Event Dataset for each country (Sundberg and Melander, 2013). Table C.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 C.5, show the same patterns as compared to our main analysis. Fourth, to deal with short-term time trends we include country-specific non-linear time trends (cubic splines) to our models. Table C.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% 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 C.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 C.8.1 - C.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 2.3 above (see Model C.8.8), while elections alone are not anymore significantly related to an increase of DoS attacks on domestic hosts (see Model C.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% of the lookups only resolve to one unique country, this statistic decreases to 64% 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 C.9 in Appendix C). 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, countries host their news websites, excluding the foreign countries where we empirically observe the true shares. Model C.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% of our collected newspaper use Content Delivery Networks (CDNs), 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 C.9.5 – C.9.6 show similar results.

Finally, we investigate a potential non-linear 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 C.10). Figure 2.5 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 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

[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, Automattic, AliCloud, CDN77, Edgecast and CacheFly.

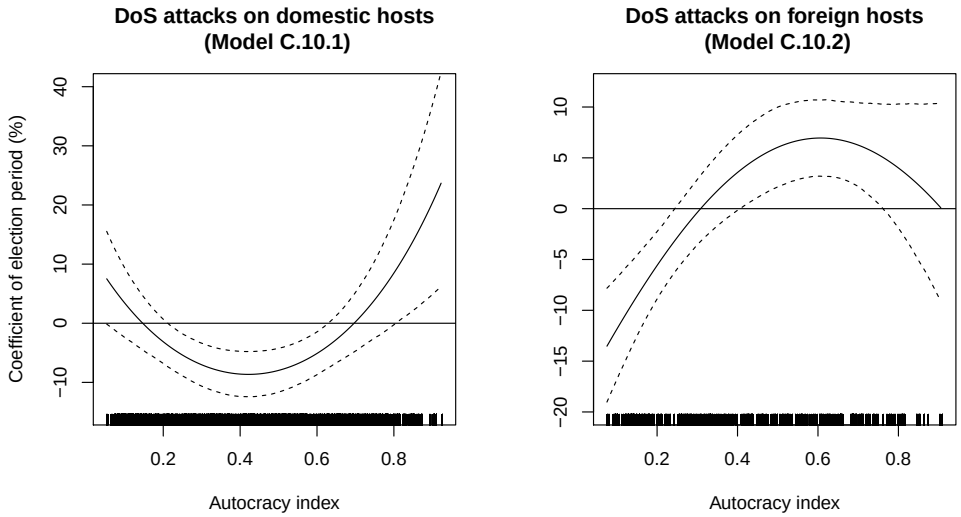

Figure 2.5: Interaction effect of election period dependent on the level of autocracy and its squared term. 95% confidence interval displayed with robust standard errors clustered at the country level. Simulations based on 10,000 draws. Observations towards the right of the panels correspond to more autocratic systems.

DoS attacks more likely as they are less costly compared to high-risk forms of collective action, e.g., 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 USA, Sweden and France appear to be (still) rather the expectation than the rule.

2.6 Conclusion

In this paper, 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 government-related 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 non-democratic 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?

3

Hot Topics: Denial-of-Service Attacks on News Websites in Autocracies

Abstract: Most authoritarian countries censor the press. As a response many private and independent news outlets have found refugee in the Internet. However, despite the global character of the Internet, news outlets are also vulnerable to censorship and repression in the cyberspace. This study investigates the motivation for Denial-of-Service (DoS) attacks on news websites. I propose that DoS attacks can follow two censorship mechanism: (1) attackers use them to temporally disable complete websites and censor content just-in-time and/or (2) send repressive signals to news outlets after they reported about sensitive news. For the empirical test, I monitored the status of 19 non-state Venezuelan news websites from November 2017 until June 2018 and retrieved their first page headlines every day. Using topic models for short text and rare event logit regression models show that the use of DoS attacks as a just-in-time censorship tool is limited. Rather, these attacks are used to punish news outlets for their reporting on unwanted news. This study deepens our understanding of how authoritarian governments use modern technologies as means for repression and censorship.

3.1 Introduction

One tactic for authoritarian governments to stay in power is to control and censor the press (Wintrobe, 2000; Frantz and Kendall-Taylor, 2014). 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 evade censorship and still reach domestic and global audiences. However, even in this global network, news outlets are vulnerable to censorship. 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 only received little academic attention so far.

According to anecdotal evidence one type of cyberattacks, so-called Denial-of-Service (DoS) attacks, frequently targets news and other websites during sensitive times in authoritarian regimes (Cardenas, 2017; Global Voices, 2011; Nazario, 2009). These attacks flood servers with high levels of Internet traffic, making them temporally not accessible for Internet users worldwide. For instance, when on March 4, 2019, the self-declared Venezuelan president Juan Guaidó returned to Caracas to continue his political fight against the Maduro government, several newspapers were hit by DoS attacks at the very same day (Rosas, 2019). Beyond Venezuela, reports about DoS attacks against Russian newspapers when they published an electoral fraud map 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. In fact, a recent macro level study suggests that DoS attacks are systematically used to censor during politically sensitive periods (Lutscher et al., 2020).[1] Nevertheless, it remains unclear when, why, and what newspapers are targeted. Do governments or government-related actors merely attack outlets known for criticism? Do DoS attacks occur randomly or do specific events increase their likelihood? Or is it the published news content at a specific point in time that triggers DoS attacks?

Previous works exploring these questions have relied on anecdotal evidence, which comes with two main biases. It focuses solely on the attacked website at a specific point in time (selection bias) and only considers attacks that are documented in media reports (reporting bias). This paper aims to overcome these problems by (1) focusing on several news websites over time and (2) measuring incidents of DoS attacks actively. In this paper, I monitor the status of a number of non-state news websites in Venezuela from November 2017 until June 2018.

Venezuela is not solely a relevant case to study as there have been many incidents of DoS attacks, but also because the Venezuelan government has become more authoritarian in recent years, making online outlets the only independent information source for

[1] For other politically motivated uses of DoS attacks see Lutscher et al. (2020) and Valeriano and Maness (2014).

citizens (Cardenas, 2017). Furthermore, while previous studies explored means of online censorship mainly in China (e.g., King, Pan and Roberts, 2013; Roberts, 2018), studies on competitive authoritarian regimes and on less sophisticated censoring tools are still rare.[2]

In this paper, I argue that the content a newspaper publishes at a specific point in time may increase the likelihood of DoS attacks. Either DoS attacks are used to censor sensitive content "just-in-time" and/or governments or government-related groups launch them as a repressive censorship tool. By just-in-time, it is meant that the perpetrators use DoS attacks to temporally disable the complete website when sensitive content is published. In contrast, the goal of the repressive mechanism is to punish news outlets for their actual or previous reporting on sensitive topics.

In the empirical part, I employ an inductive approach to infer topics Venezuelan newspapers report on. I decided to use this approach because it is *a priori* not known what news are censor-worthy. Afterward, I run statistical models to investigate what topics are related to a higher likelihood of DoS attacks. To distinguish between the theoretical mechanisms, I compare the results of these models looking at the development of news topics in the short- and medium-term. By definition, the just-in-time censorship mechanism can only be triggered by topics in the short-term. In contrast, actual and previous reporting on sensitive topics may be responsible for the repressive use of DoS attacks. More sensitive topics that are therefore exclusively related to the likelihood of DoS attacks in the short-term would support the use of DoS attacks as a just-in-time censorship tool. More topics appearing in the short- and medium models or medium model only support the repressive censorship mechanism.

The results show that published content seems to matter. However, only a few DoS attacks are clearly and exclusively related to a higher likelihood of DoS attacks in the short-term. These include reports about the exiled opposition, resignation (demands) and the petroleum sector. In contrast, reports on general socio-economic topics (outages, shortages, etc.), sanctions and corruption, as well as reporting extensively on Maduro increase the likelihood of DoS attacks in the medium-term. Thus, it seems that publishing sensitive news does not necessarily trigger DoS attacks on online outlets just-in-time. Instead, most news websites face DoS attacks as a repressive response and punishment for their actual or previous reporting. The study adds an important dimension to the literature on authoritarian information control as this finding may not only be valid for the use of DoS attacks but also for other means of censoring, both on- and offline.

[2] A competitive authoritarian regime is a country that holds elections, and where there is still a potentially dangerous opposition, yet, in which the government in power alters the political playing field to their favor (Levitsky and Way, 2010).

3.2 Censorship and Modern Technologies

Within the literature on autocratic politics and censorship, there is still little agreement on what censorship entails, how it works, and when it is used. One part of the literature puts forward that the primary motivation for censorship is to deter collective action against the regime (e.g., Edmond, 2013; King, Pan and Roberts, 2013; Wintrobe, 2000). Other studies show that governments repress regime-critical information that might legitimize grievances, reveal citizen's preferences and signal regime weakness (e.g., Kuran, 1991; Crabtree, Fariss and Kern, 2015; Gueorguiev and Malesky, 2019; Shadmehr and Bernhardt, 2015). Again others describe means of information control and repression as a tool to depoliticize the population in general (Geddes and Zaller, 1989) or indoctrinate the whole population with a regime's ideology (Friedrich and Brzezinski, 1965). Recently, Roberts (2018) proposes that censorship works through three different but non-exclusive mechanisms: fear, friction, and flooding. Fear deters media institutions and individuals to distribute and consume information by threatening repercussions. Friction increases the costs for individuals to gain access to information but also to distribute it. Flooding increases the relative costs of competing information and creates distractions by distributing pro-regime messages, for instance.

State censorship in the 20^{th} century meant that authoritarian regimes aimed to control national newspapers, radio and TV stations. While this is still true in the 21^{st} century, the digital age brought both challenges and opportunities for authoritarian regimes related to information control. Whereas a decade ago modern information- and communication technologies was praised as liberation technology (Diamond, 2010), other studies highlight that these technologies have largely expanded an authoritarian government's toolkit for censorship and repression (Deibert and Rohozinski, 2010; Hellmeier, 2016; Roberts, 2018). Governments have several options to censor the Internet. Here, one can mainly distinguish between legal and technical ways.[3] First, many countries restrict the access to websites by law and force their internet service providers (ISPs) to block these websites. This form of online censorship that often targets pornographic and gambling websites is usually public, meaning when users open a respective website there is a disclaimer that access to the website is forbidden. Second, authoritarian governments employ a vast range of more or less sophisticated technical measures to restrict the access to sensitive websites and social media content. This can happen either temporally or permanently, as well as publicly or covertly (cf. Deibert et al., 2008; Deibert and Rohozinski, 2010).

The body of the empirical literature on online censorship is still relatively small. This stems from the fact that censorship is (1) hard to measure (Roberts, 2018) and (2) many censoring tactics are not yet explored due to the rapid change of the Internet.

[3]For completeness, authoritarian governments also increasingly engage in a so-called 'networked authoritarianism," harassing opposition bloggers, setting up pro-government websites and using social media for propaganda and distraction purposes (e.g. Pearce and Kendzior, 2012; Munger et al., 2018).

Hellmeier (2016) finds in a macro level study that Internet censorship is positively related to political unrest and regional instability in authoritarian regimes. Computer science studies show that websites, which topics include pornography, social media, music websites and, very broadly, regional news, are more likely censored (Pearce et al., 2017; Weinberg et al., 2017). Closer to censoring dynamics, King, Pan and Roberts (2013) illustrate that the Chinese government quickly censors social media posts when they have a collective action potential. In contrast, posts that criticize the government are not systematically censored. In a recent study, Gueorguiev and Malesky (2019) question this conclusion. The authors show that the analyzed sample of social media posts largely coincided with a state-led consultation campaign encouraging criticism on policy proposals. Other studies on China (King, Pan and Roberts, 2017), Venezuela (Munger et al., 2018) and Russia (Spaiser et al., 2017) examine yet another government strategy empirically. These studies show that governments try to shift social media discussions away from sensitive issues.

Finally, in a recent macro study Lutscher et al. (2020) suggest that authoritarian governments also use cyberattacks as tool to censor in the online sphere. More precisely, the authors propose that governments use DoS attacks to censor sensitive websites, as well as that activists launch DoS attacks as a form of protest against repressive governments. Using new data to measure DoS attacks inferred from Internet traffic data, the study finds that the frequency of DoS attacks increases during election periods in competitive authoritarian regimes. In particular, the number of DoS attacks increases against servers in countries where the authoritarian regimes' newspapers are hosted. Although this evidence supports a censorship use of DoS attacks, it has not yet been investigated when, why, and for what purposes specific news websites are attacked in non-democratic countries.

3.3 DoS Attacks on News Websites

I propose that the censorship use of DoS attacks on news websites in autocracies can follow two mechanisms. First, governments and/or government-related groups launch DoS attacks to temporally and completely disable a website and make access to sensitive information more difficult, what I refer to as "just-in-time censorship."[4] Second, perpetrators employ DoS attacks against outlets to punish them as they reported on sensitive news, a mechanism I call "repressive censorship."

First, DoS attacks launched for just-in-time censorship overload targeted websites, exactly when news outlets published regime-threatening material. Following the framework by Roberts (2018), DoS attacks are useful for increasing friction costs, making it harder for citizens and the global audience to find sensitive information. An average

[4]Deibert and Rohozinski (2010) use this term referring to online censoring tools that allow to control content just in time.

Internet user only sees that the website is not accessible or loads very slowly. The user does not know that the website was targeted by a DoS attack to censor and would not spend extra efforts to search for the reasons of the outage. Several studies show that, when it comes to information consumption in the digital age, the average consumer is extremely impatient and will visit other websites if they have to wait longer (Athey and Mobius, 2012; Brutlag, 2009, cited by Roberts 2018, p.77). Politically engaged individuals might notice that the website was taken offline on purpose and would invest more time and costs to find out why. However, for authoritarian governments, the main goal to censor may not be to restrict information for the critical citizen per se but to make it more difficult for the majority of people to receive sensitive information (Roberts, 2018; Hobbs and Roberts, 2018). Moreover, attacks do not only increase friction costs for citizens and the global audience but also for news providers because they are forced to invest in counter-measures if they want to still provide their content. They have to employ IT experts, hire DoS mitigation services, or look for alternative ways to provide information, which may cost up to several thousand US dollars depending on the measure.

Second, DoS attacks as a repressive censorship tool follow a different logic. Here, the main goal is not to hinder the spread of information just-in-time but to punish news outlets for what they reported previously. In addition to the inability of news websites to provide news when DoS attacks hit them, they also experience a loss in revenues. This is because no user sees their advertising, which constitutes the primary income for online outlets (Mitchelstein and Boczkowski, 2009). Moreover, website shutdowns signal that information from the attacked website is not reliable, especially when websites are frequently offline (Klyueva, 2016, pp.4667f). This factor might lead to fewer visitors and financial losses in the long run. Apart from economic considerations and questions of trust, DoS attacks have also a psychological component creating fear among news website owner and journalists (cf. Roberts, 2018). DoS attacks can be understood as a repressive signal to the outlet to be careful what to report on and may lead to self-censorship in the future. In fact, experiments show that cyberattacks increase an individual's feeling of vulnerability and stress levels (Gross, Canetti and Vashdi, 2017).

From the perspective of authoritarian governments, DoS attacks are convenient as they are low-cost and quickly employed. Even governments that are not very tech-savvy can "outsource" DoS attacks to government-related groups or rent botnet servers to conduct attacks (Lutscher et al., 2020). While state actors have the highest motivation to launch DoS attacks on outlets, it may also be that patriotic hackers mount attacks on independent news outlets if they disagree with specific articles (cf. Deibert, Rohozinski and Crete-Nishihata, 2012). Additionally, outlets can be targeted even when they host their server abroad, which more critical newspapers usually do.[5] Another advantage is

[5]This is not the only reason. Other reasons include better network infrastructure and support in technologically advanced countries.

that DoS attacks often go unnoticed, which is useful in increasing friction costs as the average user would not notice that censorship is at work. Finally, even if attacks are observed publicly, they are hard to trace back. Governments can deny involvement and save reputational costs. All these points make the use of DoS attacks to censor unwanted news especially useful for competitive authoritarian regimes that often want to preserve the image of being democratic and may not have the capabilities to use full-fledged methods of censorship (Lutscher et al., 2020).

The reason why we do not see DoS attacks on news website all the time is that these attacks, just like other censorship tools, also come with their costs. Although attacks are inexpensive, employing them constantly would nevertheless cost money. More importantly and as already highlighted, websites can also protect themselves from DoS attacks, which would make it more difficult and expensive to attack them constantly (cf. McAdam, 1983). In addition to these factors, DoS attacks may lead to a backlash effect, particularly when they are launched for a longer period. Citizens may find out that there is a reason for a website's outage and potentially gain more interest in the attacked website than less (cf. Martin, 2007). Lastly, constant censorship of news websites would also restrict the government to gather information on regime performance and popularity (Wintrobe, 2000, p. 20).

When should we then expect the launching of DoS attacks on news websites? An alternative mechanism would be that attacks occur independently of a newspaper's content at a specific point in time. This means it is either the nature of the newspaper, as it is known to be critical, and/or real-world developments that lead to DoS attacks. In contrast, the theoretical considerations outlined above suggest that content and especially timing matter when it comes to the different censorship functions of DoS attacks. While for the just-in-time censorship mechanism the goal is to prevent the spread of sensitive information relatively fast, the response time for the repressive use of DoS attacks could be longer. Nevertheless, to ensure that news outlets understand this repressive signal, it is plausible to assume that DoS attacks are launched relatively soon after the outlet published the unwanted news. Finally, authoritarian governments should have higher incentives to launch DoS attacks when the sensitive news are the most salient, meaning the story of the day or reported continuously. This is because more citizens will be aware of the respective content.

Anecdotal evidence supports these considerations. On the one hand, reflecting the just-in-time mechanism, online outlets in Russia were attacked one day before the December 10 election in 2011 when they published an electoral fraud map (Global Voices, 2011). Similar attacks happened in May 2012, when newspapers reported about a large-scale protest against the inauguration of Putin (Jagannathan, 2012), or in Ecuador in 2016 when news websites reported on protests (Freedom House, 2016). More systematically, these examples illustrate that the goal of the DoS attacks has been to censor regime-threatening information just-in-time, leading to the first hypothesis:

Hypothesis 3.1 *: Publishing sensitive topics increases a news website's likelihood of being targeted by DoS attacks in the short-term.*

On the other hand, supporting the repressive use of DoS attacks, the Venezuelan news website *El Pitazo* got attacked in March 2017 after publishing several articles about vice-president Tareck El Aissami links to drug-trafficking in the weeks before (Cardenas, 2017). Other examples include DoS attacks against the Russian website *Vedomist* that criticized the Russian authorities shortly before (BBC, 2009), or DoS attacks against Belorussian media outlets one day after they ran stories about university students being forced to go to a public pro-government prayer in 2015 (Freedom House, 2016). These examples illustrate that the repressive censorship function of DoS attacks seems to apply mainly in the medium-term. Nevertheless, although I could not find anecdotal evidence for this, perpetrators may also punish outlets right away. Thus, in addition to Hypothesis 3.1, we should expect that:

Hypothesis 3.2 *: Publishing sensitive topics increases a news website's likelihood of being targeted by DoS attacks in the medium-term.*

In the empirical part of this paper, I aim to distinguish between both censorship mechanisms by comparing topics that are positively associated with DoS attacks in the short- and medium-term. When sensitive topics appear in the medium-term or in the short- and medium-term models this supports the use of DoS attacks as repression tool. Topics that are exclusively associated with an increase in DoS attacks in the short-term rather lend support to the just-in-time mechanism. A plausible assumption for this distinction to be valid is that sensitive topics do not exclusively trigger repressive DoS attacks in the short-term.

3.4 Research Design

To test my theoretical expectations, I focus on the case of the competitive authoritarian regime Venezuela (Levitsky and Loxton, 2013). I set up a server that aims to measure the occurrence of DoS attacks on several Venezuelan news websites and retrieves the websites' headlines. In the next subsection, I briefly introduce the Venezuelan case. Then, I explain in greater detail how my measurement approach works. Subsequently, I describe the scraping and processing of the news headlines and introduce the independent variables: newspaper topics. Finally, I present the merged data and describe the statistical method and different models for testing the hypotheses.

3.4.1 The Case of Venezuela

After the death of Hugo Chávez in 2013, the former vice-president Nicolás Maduro took over power. Since then, the social and economic crisis in Venezuela has been escalating

(Munger et al., 2018). In December 2015, the incumbent government lost its majority in the *Asamblea Nacional de Venezuela* (AN). To stay in power, the government answered with harsh repression, the creation of the pro-government filled Constituent National Assembly (ANC) and increased levels of press censorship. Concerning the latter, the Venezuelan government has managed to almost entirely gain control over traditional media, making it hard to retrieve critical views from print and broadcast media (Freedom House, 2017*a*; Hawkins, 2016). In response, the majority of print and broadcast media has migrated to the Internet, making news websites of particular importance for Venezuelan citizens to retrieve independent news (Cardenas, 2017). Unsurprisingly, the Venezuelan government has responded to this adjustment strategy of media outlets. It has set-up pro-government websites, uses trolls in social media (Munger et al., 2018), has banned websites by selectively using filters at the ISP level and was likely behind DoS attacks against news and other websites (Freedom House, 2017*b*; OONI, 2018).

This study focuses on the period from November 2017 until the beginning of June 2018, which includes the municipal elections, on December 10, 2017, and the presidential election on May 20, 2018. Here, Nicolás Maduro was able to win with almost 70%, yet it was characterized by a ban of opposition candidates beforehand, a boycott by most of the opposition, the lowest voter turnout in Venezuelan history and accusations of electoral fraud (Sen, 2018).

3.4.2 Measurement of DoS Attacks

Previous studies on DoS attacks emphasize that, especially in authoritarian regimes, DoS attacks on civil society and news websites are often under-reported and go unnoticed (Hardy et al., 2014). To counter this reporting bias, I use an active measurement approach.[6] For this purpose, I set up a server that monitors the online status of national news websites in Venezuela in real time. The list of websites comes from www.abyznewslinks.com, a website that gathers news websites worldwide. Because I am only interested in DoS attacks that aim to censor and are likely conducted by the government or government-related groups, I restrict the sample to websites that are not clearly associated with the state.[7] Besides, I do not consider news websites that did not update content, where content could not be downloaded, purely aggregate news from other websites and websites that were published in English, leaving me with 19 websites. For a full list refer to Table D.1.1 in Appendix D.1.

In order to understand the measurement approach, it is necessary to know how devices communicate via the Internet. In a nutshell, devices communicate on the Internet in the way that a client A sends a request to a host B, this host B then responds to this

[6]Other public data sources on DoS attacks that circumvent this problem, e.g., passively measured attacks from Internet traffic (CAIDA, 2016), are unfortunately available on the country level only.

[7]Government associated news website were identified by ".gob" addresses and government symbols within websites. In addition, I consulted a country expert, Miguel Latouche.

request and, if acknowledged, enables client A to communicate with the server, e.g., see a website. In the case of web servers, this communication follows the so-called Hypertext Transfer Protocol (HTTP) where hosts (web servers) answer with a standardized numeric response code to the request made by the client. When the web server returns a "200" status code, the connection can be established. If not, some error likely occurred. Error codes with a "4XX" number indicate that the client (my server) has problems to reach the host, whereas "5XX" codes mean that the web server where the news website is hosted encounters problems. Since the average duration of DoS attacks ranges between 18 and 48 minutes (Jonker et al., 2017), my server contacts the Venezuelan news websites every 30 minutes and saves the returned status code.[8] In addition to the standardized codes, my script returns the code "999" when the script cannot open the respective website. This may occur due to errors on the server side or when the host detects the automated request through my script.

In classifying DoS attacks, I focus on HTTP codes returning a 503 error code that indicates that the server is currently unavailable, most likely caused by an overload in traffic. In essence, this is the main observable consequence of a DoS attack. I code a newspaper/day as attacked, when at least one measurement failed. Additionally, I consider the error codes 522 and 524 that are returned when Cloudflare, a DoS mitigation service, cannot connect to the original server as it is likely overloaded. Besides, servers protected by Cloudflare service also return a 503 error code when the server is put "under attack" mode, enabling to capture attack attempts for these cases as well.

Apart from external attacks, there might be other reasons for a server outage or overload. For example, an unstable electricity/Internet network or maintenance work might cause an outage. A domain look-up shows that almost all of the monitored websites are hosted abroad at some big data center or protected by Cloudflare or other services.[9] Since most servers are hosted abroad, unstable electricity or Internet networks are unlikely to be responsible for an outage, which is an actually frequent issue within Venezuela. Furthermore, because major service providers conduct scheduled maintenance work in the period from 0 - 6 a.m, I do not consider measurements within this time-span to reduce false-positives (Richter et al., 2018). In later sensitivity checks, I consider the return of other 5XX and 999 error codes also as potential DoS attacks, focus on longer attacks, as well as discuss the limitations of my measurement in greater detail.

Figure 3.1 shows the newspapers' status for the period from November 13, 2017 until June 03, 2018. The figure highlights that nine websites suffered from DoS attacks at least once and that in total 47 incidents of attacks occurred. Frequently affected websites are

[8] I further restricted the measurement to every 30 minutes as constant requesting would lead to a blocking of my server. Another approach is to capture ping times, which is the time a request takes. Concerning this approach, many of the monitored servers are protected and not "pingable."

[9] For the look-up I used OpenINTEL (van Rijswijk-Deij et al., 2016). Protection by DoS mitigation services does not necessarily mean that DoS attacks cannot be successful. They still can when they extend the "protected" bandwidth or exploit other server weaknesses.

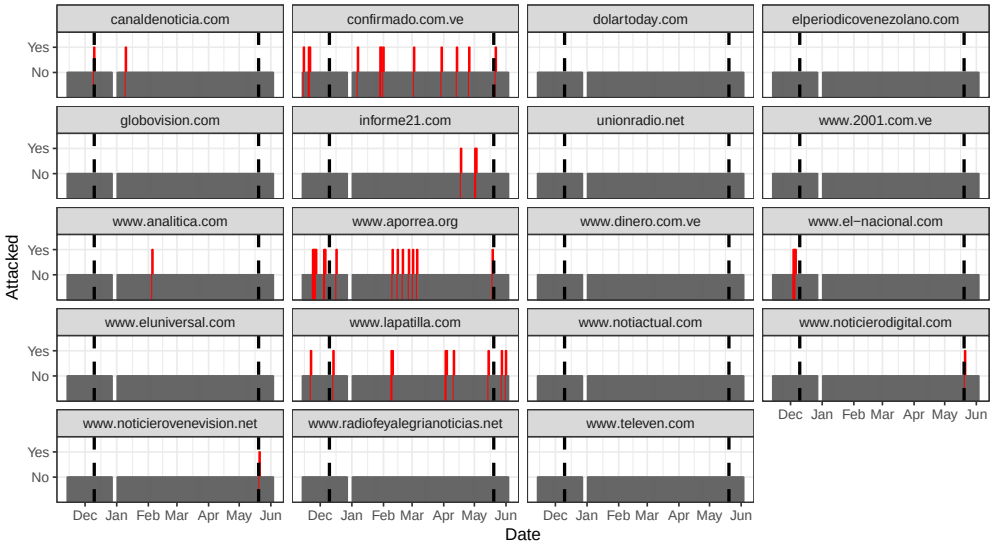

Figure 3.1: Incidents of measured DoS attacks in Venezuela November 2017 - June 2018. Note: The two vertical lines show the municipal election (December 10, 2017) and presidential election (May 20, 2018). Blank periods indicate time periods where the measurement did not work.

Aporrea.org a leftist opposition news website that was formerly loyal with the Chávez regime, as well as the critical news outlets *La Patilla* and *Confirmado*. Furthermore, the figure shows some attack cluster against multiple websites around the municipal and presidential elections. Both observations suggest that DoS attacks more often target critical news websites and that external events do increase the likelihood of DoS attacks (cf. Lutscher et al., 2020). Regarding the attack duration, an average attack lasted around 1,5 hours (three failed measurements), while the median is slightly above 30 minutes, one failed measurement (see Figure D.1.1 in Appendix D.1).

3.4.3 News Retrieval and Topic Modeling

To retrieve the content of the websites, I download the first page of every website every day at 01:00 p.m. Venezuelan time using the *urllib2* and *BeautifulSoup* libraries in Python. Afterward, I custom tailor the extraction of headlines, including the first paragraph, if available, for each different website. In this process, I ignore uninformative headlines with less than three words, and, when the website is structured according to broader categories, news on entertainment, sport, culture, and technology.[10] As pre-processing steps, I remove punctuation and numbers (dates, etc.), use lower-casing and Porter stemming of the tokens, as well as remove Spanish stopwords and other newspaper-related words (day names, "read more" buttons, authors, etc.) that do not contribute to the later analysis. I do not remove infrequent terms as the content that

[10]This was not possible for all websites as some had no clear structure (see Table D.1.1 in Appendix D.1).

might trigger DoS attacks might be rare. Table 3.1 reports the summary statistics for the textual data.

No. of website/days	No. of headlines	Avg. no. of headlines per website/day
3566	123889	34.74

Avg. term length per headline	Std. dev. term length per headline	Total no. of stemmed terms
13.14	9.41	26640

Table 3.1: Summary statistics of text corpus.

To investigate whether news topics are related to DoS attacks, it is first necessary to reduce the high dimensionality of the textual data. Since it is not necessarily clear what topics are sensitive, I use topic model approaches to link the headlines to broader topics. The most commonly used topic models are Latent Dirichlet Allocation (LDA) models (Blei, Ng and Jordan, 2003). The main idea is that each document is a combination of a small number of topics. LDA models are looking for co-occurrences of words in the same text (word-document co-occurrence), define them as topics, and discriminate between documents by applying Bayesian learning. The problem is that these models perform rather poorly with short text where words often only appear once in every document. To reduce this problem, experimental evidence in computer science has shown that the best performing approaches are models that do not look at each term separately but look at word embeddings (Yan et al., 2013; Xun et al., 2016; Shi et al., 2018).

I use the approach taken in Yan et al. (2013) that enables to link the generated topics with a certain probability to specific headlines. This so-called Biterm Topic Model (BTM) does not look at word-document co-occurrences but learns topics by modeling word-word co-occurrences patterns in the whole corpus.[11] For example, when the words economy, recession, and crisis frequently co-occur in headlines (irrespectively where and in what order), the algorithm identifies these terms as belonging to the same topic (for more details see Yan et al., 2013).

As with other unsupervised topic models, it is necessary to specify the number of topics (K) in advance. I decided to set $K = 50$ as a good trade-off between the level of aggregation and specificity for each topic. 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 the topics (see Appendix D.2). For the algorithm to run, one has to define the conjugate priors α and β. I follow the specification in Yan et al. (2013) for short text by setting $\alpha = 50/K$ and $\beta = 0.01$. The algorithm is then run using Gibbs sampling for 2,000 iterations.

As the last step, I label each topic by interpreting the top 15 terms per topic.[12] Table

[11] For the most recent approach by Shi et al. (2018), I was not able to link the topics back to the respective headlines. The other algorithms rely on external data to create word embeddings (Xun et al., 2016); data which I do not have for newspapers in Venezuela.

[12] In a reliability check, a second coder linked the terms to the identified labels. The overlap is 90%. The mismatch stems from economic topics that are harder to distinguish and as shown in Figure D.1.2

3.2 shows the ten most frequently appearing topics. The 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 in these top 10 topics is that the monitored news websites report on worldwide news but unsurprisingly mostly about issues within Venezuela.

P(z)	Label	Top 5 words
0.066324	General opinion	Venezuela, continue, can, Venezuelan, politics
0.043895	Sanctions	Venezuela, USA, sanction, United, government
0.041180	National assembly	national, assembly, dispute, president, AN
0.040474	Maduro	Maduro, president, Nicolas, Venezuela, government
0.039453	Opposition candidate	Falcon, candidate, presidential, Henri, election
0.038004	Government-opposition dialog	dialog, government, opposition, Venezuelan, Dominican
0.035994	Election	election, electoral, presidential, CNE, national
0.033783	Migration crisis	Venezuelan, country, Venezuela, Colombia, crisis
0.031420	Protest/shortages	protest, San, missing, municipal, city
0.031162	Óscar Pérez	Pérez, Óscar, killing, body, officials

Table 3.2: Top 10 identified topics. 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.

To investigate whether the estimated topics are valid, I first look at semantic validity, checking whether the generated topics are coherent and overlap with the respective headlines. Second, I also focus on predictive validity, investigating whether the assigned headlines reflect real-world developments (Grimmer and Stewart, 2013; Quinn et al., 2010). The semantic evaluation confirms that the model performs quite well in finding coherent topics (see Table D.2.1 in Appendix D.2). For the predictive validity, I plot the temporal development of some topics linking them to real-world events. The following figures show the temporal development of the relative proportions of the topics election (Figure 3.2) and Óscar Pérez (Figure 3.3) aggregated across all newspapers. For Figure 3.2, the relative topic proportion increases sharply close to the election dates on December 10, 2017, and May 20, 2018. In February 2018, the National Electoral Council (CNE) decided about the ban of several candidates, which is reflected by the slight increase during this period. In Figure 3.3 one can see that the highest proportion of the topic is in mid-January after a special commando killed Óscar Pérez in the so-called *El Junquito* raid (Casey, 2018). Overall, these tests make me confident that the results of the BTM are valid.

3.4.4 Data

To merge the dependent and topic variables, I define a day lasting from 1 p.m. until 1 p.m. the next day to ensure that the potential attack happened after I downloaded the content. Then, I aggregate the generated topics to their average proportion on the daily

in Appendix D.1 highly correlated.

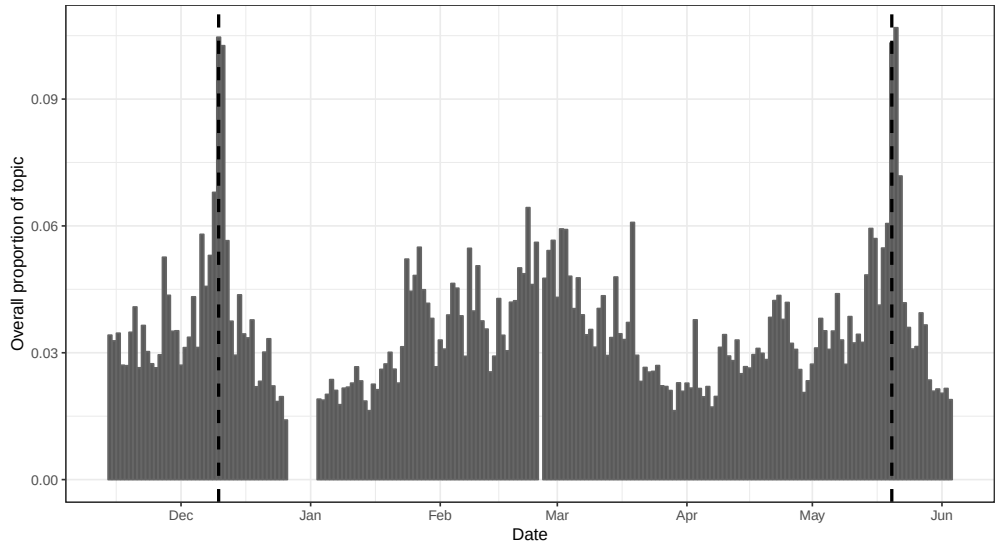

Figure 3.2: Temporal development of the aggregated topic election. Note: The two vertical lines show the municipal election (December 10, 2017) and presidential election (May 20, 2018).

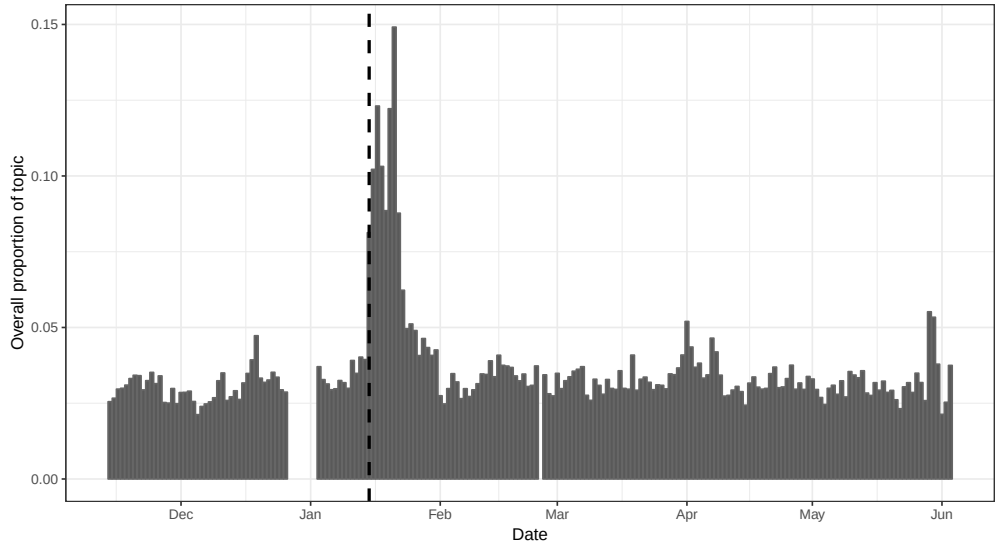

Figure 3.3: Temporal development of the aggregated topic Óscar Pérez. Note: The vertical line corresponds to the killing of Pérez on January 15, 2018.

newspaper level as authoritarian regimes should have higher incentives to censor content when the sensitive topic is the most salient. In later sensitivity tests, I also aggregate the topics to the maximum proportion of a topic, i.e., assuming that it matters more whether the newspaper reports at all about a specific topic.

Figure D.1.2 in Appendix D.1 shows the pair-wise correlations of all topics and websites for the newspaper/day aggregation. The figure points to a large cluster of collinear topics about economic issues: *financial market*, *recession*, *Spanish development aid*, *investment* and *economy opinion* with pair-wise correlations above 0.8 (top-left corner). Because these topics are additional highly correlated to one specific website (*dinero.com.ve)*, I do not consider them in the main specification that includes newspaper fixed effects.[13] Furthermore, three other topics (*investment/infrastructure*, *leftist opposition* and *indigenous groups/diseases*) are highly correlated to specific newspapers and are therefore not considered in the main specification. Although other topics do not correlate that strongly, some of them show significant correlations. When interpreting the later empirical results, this observation has to be kept in mind.

3.4.5 Method

For the analysis, I use a penalized logistic regression with a Firth bias correction (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, Hays and Franzese, 2018). In a recent paper, Cook, Hays and Franzese (2018) show that this correction allows to include fixed effects as well as to retrieve accurate marginal effects of the predictors, making it ideal to use for the present study. I run the models separately for each topic to avoid problems of over-fitting and saturation that can lead to biased estimates especially in cases with few events (Vittinghoff and McCulloch, 2007).[14]

I set up four different specifications that all include a lagged dependent variable to control for serial correlation. First, I use pooled models that include the respective topic variable and a variable measuring the number of headlines published for the respective outlets. I add the latter variable as the absolute number of headlines also influences the mean topic proportion per newspaper/day. Second, I include newspaper fixed effects as the nature of the news website might increase the likelihood of being attacked and determines news reporting. By this, I also control for the different levels of DoS protection news websites have. Furthermore, temporal events have an impact on what is being published and might also directly influence the likelihood of DoS attacks, e.g., closeness to elections (Lutscher et al., 2020). Thus, in a third and fourth specification

[13] As well as only the topic *recession* in the pooled specification.

[14] Vittinghoff and McCulloch (2007) argues that that at least 5 events per predictor variable are sufficient. However, it is also necessary to include potential confounders to the analysis. That is why I include newspaper and temporal fixed effects. Running models including all topics and fixed effects do not converge.

I add temporal fixed effects on the week and day level, respectively.[15] In the fixed effects specifications, I leave out the number of headlines variable as the newspaper fixed effects should capture this variable. All models come with robust clustered standard errors for each website to take into account heteroskedasticity in the error term. The full specification is summarized in the following equation:

$$Logit(DoS_{i,t}) = \beta_0 + \beta_1 topic_{i,t} + \beta_2 DoS_{i,t-1} + \gamma_i + \delta_t + \epsilon_{i,t}. \tag{3.1}$$

where γ_i includes the newspaper fixed effects, δ_t the respective time dummies and ϵ_{it} represents the error term.[16]

To investigate Hypothesis 3.1, which says that sensitive content attract DoS attacks in the short-term, I measure the independent and dependent variables on the same day t, while ensuring that the topics appear temporally before the attack. For Hypothesis 3.2 that expects a medium-term impact of topics on the likelihood of attacks as well, I calculate the average proportion for each topic up to 7 days before for each newspaper-day, leaving out the topic distribution at time = t.[17] In later robustness checks, I use different thresholds for the short- and medium-term models.

To investigate what censorship mechanism is more applicable, I compare topics that are significantly and positively related to an increase in DoS attacks in both models. When sensitive topics appear in the medium-term or the short- and medium-term models this supports the use of DoS attacks as a repression tool. In contrast, topics that are exclusively associated with an increase in DoS attacks in the short-term rather support the just-in-time mechanism. As stated above, I assume that sensitive topics do not exclusively trigger repressive DoS attacks in the short-term.

3.5 Results

This section starts by discussing the results of the short- and medium-term models. Then, I discuss potential differences between both time frames and introduce some ad-

[15] To improve convergence and efficiency, I follow Cook, Hays and Franzese (2018) and only add dummies/intercepts for weeks and days that experienced a DoS attack. I proceed like this because days without DoS attacks do not add additional information to the model and can be therefore aggregated to a baseline. For the newspaper fixed effects, I include all newspapers to control for differences in the mean proportions that are due to the number of headlines (excluding one newspaper as baseline category).

[16] Alternatively, one could use matching procedures to find similar observations that only differ in one specific topic. However, for this approach, first, one would have to identify spikes in topic developments, and second, one could only control for time or unit-specific factors but not both. From a theoretical viewpoint, the controlling of both makes more sense as the reporting on news content, and the occurrence of DoS attacks are dependent on the newspaper and temporal developments. Still the fixed effects models assume that no idiosyncratic factor is influencing both, newspaper reporting and the occurrence of DoS attacks at a specific point in time.

[17] I decided to use 7 days as threshold as from a theoretical viewpoint a repressive response should occur relatively close to the publishing date of critical news. Since the scraping of websites sometimes did not work, I take the average after removing NAs. Figure D.1.4 in Appendix D.1 shows periods in which the scraping failed.

ditional models. Finally, I point to the limitations of this study.

3.5.1 Main results

To ease the interpretation of the results, I order the generated 50 topics according to broader categories. Table 3.3 shows this classification for all topics and I discuss this manual clustering in Appendix D.3 in detail. To investigate the topics that are related to a higher likelihood of DoS attacks against news outlets in the short and medium-term, I simulate the average marginal effects for all topics that are positively and significantly related ($p<0.05$) to the likelihood of DoS attacks in at least one of the fixed effects specifications. The complete results for all models are summarized in the Tables D.1.2 - D.1.9 in Appendix D.1. The panels in Figure 3.4 (short-term models) and Figure 3.5 (medium-term models) show these average marginal effects sorted along the seven broader categories combined in one graph. The simulations display the "effect" of moving the share of the respective topic from its minimum to its maximum value, i.e., reporting nothing at all to reporting extensively about the topic.

Category	P(z)	Topics
Social/economic crisis	0.272	Migration crisis, petroleum, salary/prices, shortages healthcare, exchange rate, shortages, outages, child mortality, PDVSA, airline (opening/closing), [indigenous groups/diseases], mining/sport (mixed), [recession], [economy opinion], work opinion, [investment/infrastructure], [investment], [Spanish development aid], [financial market]
Legitimacy	0.197	Sanctions, national assembly, international organizations, court sentences, resignations, corruption, exiled opposition, [leftist opposition]
Other	0.146	General opinion, education studies, music/entertainment, weather, earthquake/accidents, church/job offer (mixed)
Government	0.142	Maduro, government-opposition dialog, government ministers, food policy, economy policy, cryptomoney, regulations
Protest/repression	0.097	Protest/shortages, Oscar Perez, political prisoners, military
Election	0.075	Election, opposition candidate
International	0.071	Russia, Colombia border, USA/Korea, Cuba

Table 3.3: Categorization of topics. Note: P(z) = distribution over whole corpus. Highly collinear topics are not included in the main analysis (within square brackets). See Appendix D.3 for the discussion of the categorization.

Short- and Medium-Term Models Both figures highlight that the marginal effect of a number of topics is different from zero. Seven topics show positive and significant marginal effects at a 95% level in the short-term when day fixed effects, that is the most rigorous specification, are included. When looking at the medium-term development of topics this is the case even for eight topics. Furthermore, the majority of these topics appear to be politically sensitive.

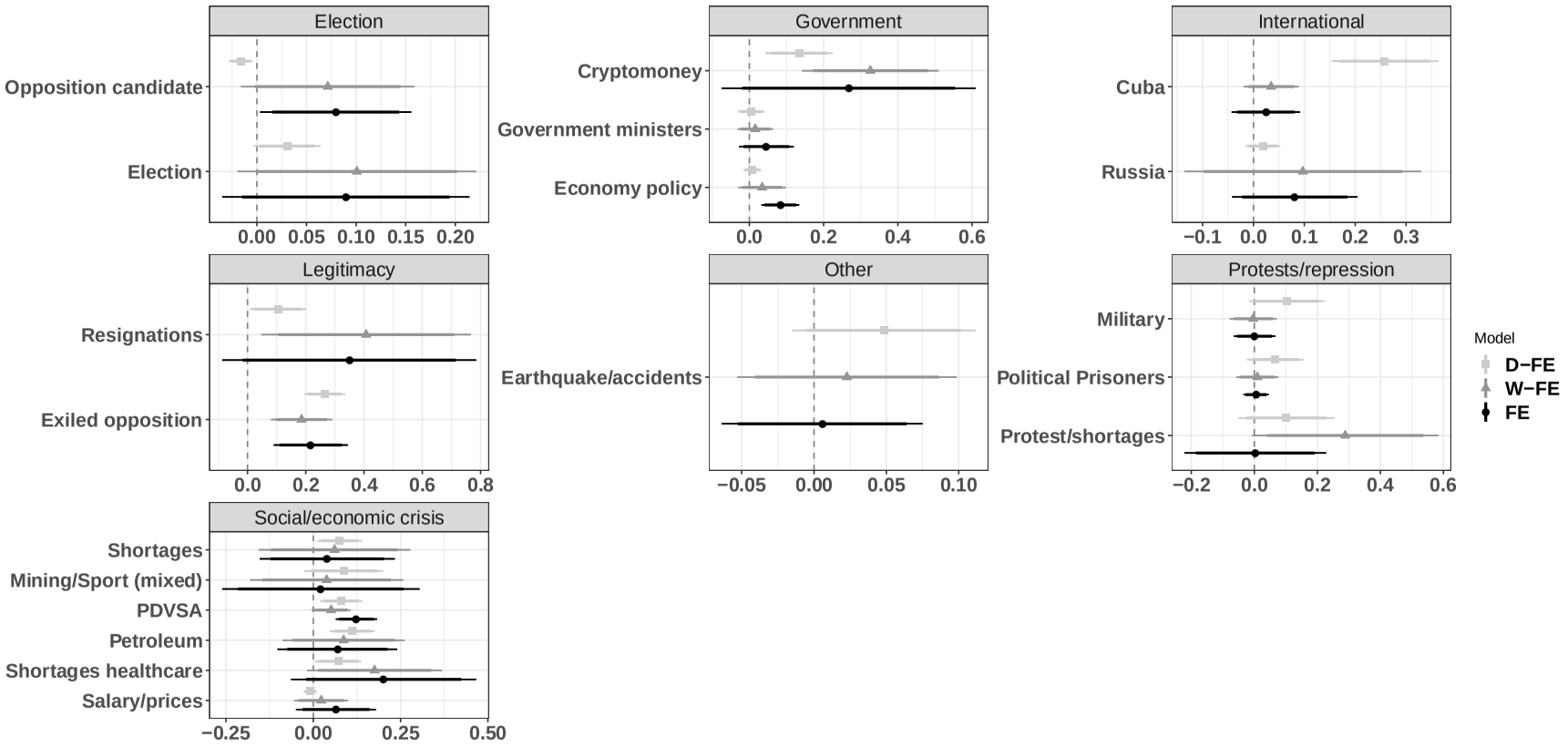

Figure 3.4: Average Marginal Effects (AME) of significantly positive related topics (short-term models) on a news website's likelihood of receiving DoS attacks. Note: Each AME is calculated in separate models. Simulations based on 1000 draws. Topics are calculated in individual models and combined in the figure. D-FE = day and newspaper fixed effects, W-FE = week and newspaper fixed effects and FE = newspaper fixed effects. The topic *Cuba* and *cryptomoney* are highly correlated to specific websites.

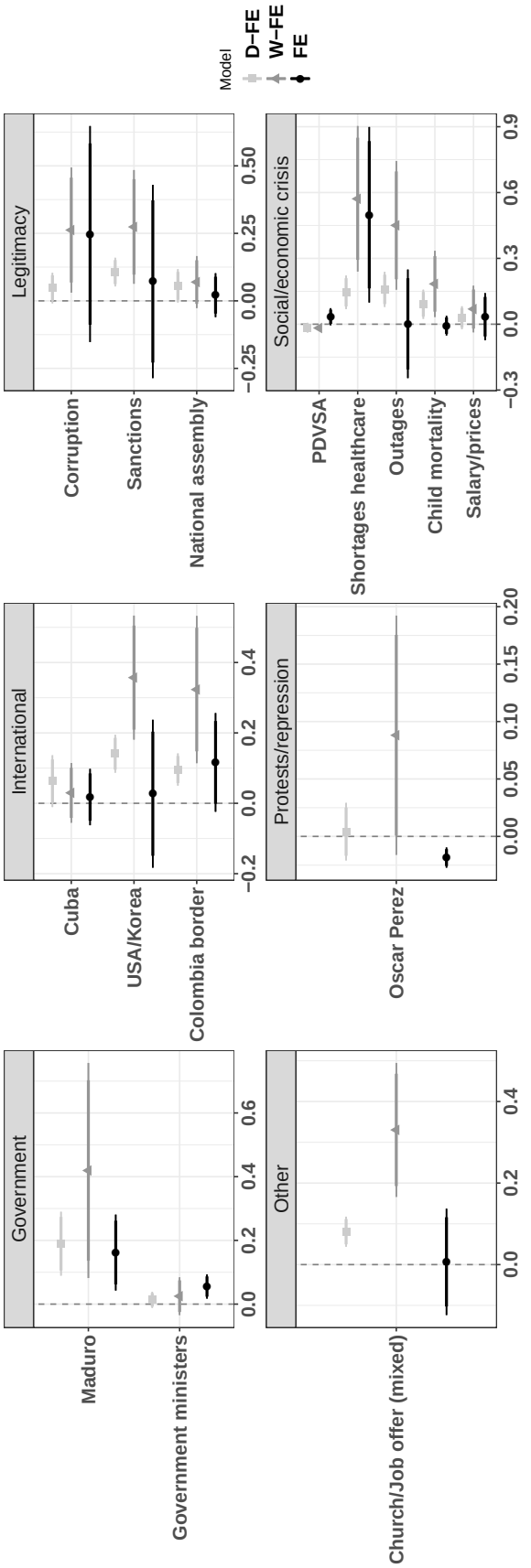

Figure 3.5: AME of significantly positive related topics (medium-term models) on a news website's likelihood of receiving DoS attacks. Note: Each AME is calculated in separate models. Topics are calculated in individual models and combined in the figure. Simulations based on 1000 draws. D-FE = day and newspaper fixed effects, W-FE = week and newspaper fixed effects and FE = newspaper fixed effects. The topic *Cuba* is highly correlated to one specific website.

For the short-term models reported in Figure 3.4 these are topics related to the socio-economic crisis and legitimacy category. For the former, in particular the reporting about the state-owned oil and natural gas company *PDVSA* and *petroleum* in general as well as the topics *shortages* and *shortages healthcare* show significant positive marginal effects on the likelihood of DoS attacks. For the latter, the topic *exiled opposition* is associated with an increase up to 30% in the likelihood of DoS attacks in the short-term (compared to not reporting at all on this topic). This topic is primarily concerned with Antonio Ledezma, the ex-mayor of Caracas, who urges other governments to take action against the Maduro government. Additionally, the marginal effects of the topic *resignations* of other head of states and resignation demands – including Maduro's – is robustly related to an increase in the likelihood of DoS attacks. Finally, for the topic *Cuba* it is not necessarily clear why this should increase the likelihood of DoS attacks in the short-term. Perhaps the Cuban political system was criticized which may explain the found patterns.[18]

For the medium-term model, topics from more distinct categories display significant positive marginal effects. These are news topics dealing with the socio-economic crisis, legitimacy, as well as government and international news. First, the socio-economic related topics *shortages healthcare*, *outages* and *child mortality* display significant and positive marginal effects. Concerning the legitimacy topics, in particular the topic *sanctions* is clearly related to a higher likelihood of DoS attacks in the medium-term.[19] In addition, Figure 3.5 reveals a strong and robust finding for the topic *Maduro*. Finally, the international topics *USA/Korea* and *Colombia border* display significant findings. Although it is not necessarily clear why these topics should trigger DoS attacks, it might be that newspapers are punished when reporting extensively about the USA and Colombia, countries that do not enjoy high levels of popularity in the Venezuelan government. In addition, at least the *USA/Korea* topic correlates considerably to the *sanction* topic, which may explain the found pattern as well. Lastly, the topic *church/job offer (mixed)* seems to increase the chance of DoS attacks in the medium-term, which might be explained by the more critical stance of the church in recent years.

For the topic *cryptomoney*, which shows significant patterns especially in the short-term models, it is not really clear why it could be politically sensitive. However, since the topic is highly correlated to the website *dinero.com.ve*, with a pair-wise correlation of 0.7, respectively, it is very likely that the remaining variance does not reflect the actual topic and the finding appears to be an artifact of the statistical estimation.

[18] Other politically sensitive topics that nearly miss conventional levels of significance when including day fixed effects are found within the protest and election categories.

[19] The remaining two topics, *corruption* and the opposition-filled *national assembly* just misses conventional levels of significance.

3.5.2 Discussion and Additional Models

What do these results tell us about the proposed censorship functions of DoS attacks? Overall, the results of the simulations show more potentially sensitive topics that are significantly related to the likelihood of DoS attacks in the medium-term. Since here the just-in-time mechanism of DoS attacks cannot apply, these results speak to a more pronounced use of DoS attacks as a repressive censorship tool. Supporting this point, several of the socio-economic topics are very similar in the short- and medium-term models. This suggests that when newspaper report extensively about the social- and economic crisis in Venezuela, these newspapers may receive DoS attacks rather as a punishment. In fact, as citizens within Venezuela are either way aware of the bad economic situation, there appears to be no need to censor just-in-time (cf. Rozenas and Stukal, 2019). Nevertheless, the results show that the topics *exiled opposition* and *resignations*, as well as news on the petroleum sector increase the likelihood of DoS attacks exclusively on the same day. For these topics it seems that the main motivation of the DoS attack is to censor just-in-time as they are unrelated to an increase of DoS attacks in the medium-term.

As stated above, this conclusion rests on the plausible assumption that no sensitive topic exclusively triggers repressive DoS attacks in the short-term. Other caveats may be that the just-in-time mechanism is delayed and/or that topics trigger repressive responses also after a longer time period. To test these and other concerns, I conduct several robustness and sensitivity tests (see Appendix D.4 for details). First, I consider different time frames for the short- and medium models. The results show mostly the same positively related topics as in the main models. However, the overlap between topics in the short- and medium-term becomes larger. This lends support to the conclusion from above that the repressive use of DoS attacks appears to be more pronounced. Second, it may be that websites became unavailable not due to DoS attacks but because there were to many visitors. Controlling for general interest using Google trends shows similar results. Third, supporting that specific topics matter in determining the censorship mechanism, negatively related topics show the opposite results in the short- and medium-term models for some topics. Fourth, when I aggregate topics to their maximum value, the results show substantially smaller marginal effect sizes. This finding supports the theoretical assumption that the salience of news, as measured in the main models, is more important in influencing DoS attacks. Fifth, when I use all 5XX and 999 error codes to measure DoS attacks, the results display that very few topics remain unique in the short-term. While these results suggest the use of DoS attacks as an exclusive repression tool, these measurements likely include a high number of false-positives. Sixth, I consider stronger attacks only. These attacks need more resources and signal more serious intentions, therefore, may be more likely state-sponsored. However as the number of potential DoS attacks decreases to 21 events, this increases the likelihood of estimation

errors. Overall, the results display a larger number of significant and politically sensitive topics in the short- and/or medium-term models. For example, in line with previous work on online censorship in China (King, Pan and Roberts, 2013), news on political prisoners and protest are now significantly related to the likelihood of DoS attacks as well. In conclusion, the additional models support my main conclusion and point to a just-in-time and repressive use of DoS attacks, yet the latter appears to be more pronounced.

Finally, when the main censorship function of DoS attacks is indeed to send repressive signals, one could expect that attacked websites change their reporting after attacks. To investigate this, I focus on each attacked website and attack separately and run generalized synthetic control models (Xu, 2017) to determine whether DoS attacks influence news reporting up to 7 days after the attack. These models are discussed in Appendix D.5 in greater detail. Generally, the "effect" of my measured attacks on a change in reporting of topics remains limited. This finding may be explained by several reasons. First, the measured DoS attacks are rather short. Second, because previous reporting about specific topics could have been responsible for the attacks, websites already reported less about the sensitive issue on the attack day. Third, many servers are protected by DoS mitigation services. The few changes in reporting can be mainly observed for websites that do not use these services. Besides, potential consequences may be long-term or caused by learning effects from large-scale attacks against other outlets. Future research should investigate these points more closely.

3.5.3 Limitations

The main and additional models show (1) that reporting on politically sensitive topics are related to a higher likelihood of DoS attacks on news websites and (2) that the repressive use of DoS attacks is more pronounced. Nevertheless, the methodology and approach used in this paper come with some limitations.

First, while most indications speak for a DoS attack when a 503 error code is returned, some of them might be false-positives and other reasons on the server side were responsible for the outage. While I can show that the results remain the same when controlling for general interest, my measurement is not able to measure DoS attacks directly. As a plausibility test, I contacted all websites and asked whether they experienced DoS attacks or attempts thereof. Unfortunately, only a few websites responded. This might be explained by the tense political situation in Venezuela or because websites do not want to admit that they are targeted by DoS attacks. Those websites that responded 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. Supporting the notion of repressive censorship, one website owner admitted indeed self-censoring of sensitive content as he is afraid to be attacked

or blocked.[20] Furthermore, in one case, measured attacks on the website *Informe21* on May 2, 2018, the website was down for several days, later acknowledging on their website that a cyberattack was responsible for this outage.

Second, the measurement captures only DoS attacks that lead to an overload of the server. While this may introduce the chance of missing attacks (false-negatives), my robustness tests with more liberal operationalizations of DoS attacks still find triggering topics. In addition, as highlighted above, my measurement is also able to capture attack attempts for Cloudflare protected servers as they return the code 503 when they are put "under attack" mode. Another related issue may be that my server did not contact the website server directly but ended in the cache of the website provided by a Content Delivery Network (CDNs), which are regional servers that provide a website's content. While this might underestimate DoS attacks as CDNs essentially help servers to cope with more traffic, my measurement still shows incidents of DoS attacks even in these cases (see Table D.1.1 for websites that use CDNs).

Third, the sample of news websites is restricted to websites that are included in www.abyznewslinks.com and websites for which the measurement and extraction worked. Since www.abyznewslinks.com is a worldwide news websites collector, it might miss some Venezuelan news websites and does not include newly emerged news websites, blogs, and smaller news outlets. While this could bias the results, it appears that there is no systematic logic behind missing websites. In addition, during some attack incidents, it was not possible to download the content of attacked news websites. However, as this only concerns four attacks, it is unlikely that it altered the overall results.

Finally, one of the core problems in studying cyber and DoS attacks remains their attribution. Although government(-related) actors should have the highest motivation to launch attacks against threatening news websites, my measurement can only focus on the victim and is not able to trace back the origin of the attack. I believe that the results nevertheless support this presumption as for most of the topics the government or government-related groups have incentives to use DoS attacks to censor just-in-time or repress. Furthermore, as shown by the models considering stronger attacks, the results even show more sensitive topics related to a higher likelihood of DoS attacks.

3.6 Conclusion

Whereas previous work points to a systematic use of DoS attacks as censorship tool in autocracies (Lutscher et al., 2020), this paper has explored the motivation and timing of DoS attacks against specific news websites in these regimes. Monitoring the online status and content of 19 online news outlets in Venezuela, the results (1) find that news content matters when it comes to DoS attacks and (2) point to evidence for two different censorship mechanisms of DoS attacks. The findings show that only some topics

[20] Email conversations, July 25 - August 8, 2018 (available upon request).

increase the likelihood of DoS attacks on news websites clearly on the same day, i.e., reports about the exiled opposition, resignations as well as headlines about the petroleum sector. In contrast, general socio-economic related topics, reports about sanctions, some international topics and reporting extensively on Maduro lead to a higher likelihood of DoS attacks in the medium-term.

These findings, which are supported by a number of additional analyses, point to a more pronounced use of DoS attacks as a repressive censorship tool, where news outlets are being punished for their reporting on sensitive topics. Although this conclusion should be treated cautiously because of the limitations of this study and focus on one country, this first systematic investigation of DoS attacks on news outlets helps to deepen our understanding of cyberattacks as censoring and repression tools. Cyberattacks may help authoritarian governments not only to censor information temporarily but even more to spread fear. While the ability of authoritarian governments to do so has been limited by their borders in the past, the Internet enabled them to censor and repress globally. Finally, evidence from other means of Internet censorship in Venezuela and beyond show similar patterns, suggesting that the use and motivation of other forms of censorship, both off- and online, may be comparable (OONI, 2018; Freedom House, 2018).

4

Digital Responses to Sanctions? Denial-of-Service Attacks against Sender Countries

Abstract: Cyberattacks have been portrayed as a new coercive weapon for interstate conflict. However, it remains unknown how widely these are used in response to foreign aggression such as sanctions. Do governments or government-related groups use these new tools as a digital response? This paper investigates if economic sanctions lead to an increase in Denial-of-Service (DoS) attacks on the sender country by using data on DoS attacks measured from Internet traffic. I discuss two mechanisms why this may be the case: (1) Either targeted states respond with DoS attacks to both the imposition and, even more so, the threat of sanctions as a coercive tool to gain concessions and/or (2) they are launched to voice discontent. For the analysis I run time series models from 2008 – 2016 for the United States and the European Union as most active sanctioning entities. The results show only limited evidence for an increase of DoS attacks on the sender state when sanctions are imposed. Sanction threats appear to be unrelated to the development of DoS attacks. These findings support previous theoretical work that questions the coercive use of cyberattacks and suggest that governments do not frequently use DoS attacks as foreign policy instrument.

4.1 Introduction

When the United States reinstated sanctions against Iran on November 5, 2018, CNN wrote that US banks prepared themselves for anticipated cyberattacks (Pagliery, 2018). Several years earlier between 2011 and 2013, presumably Iranian actors had indeed launched large-scale cyberattacks against US financial and government websites supposedly in reaction to sanctions issued against Iran (e.g., Perlroth and Hardy, 2013). More precisely, the attackers used so-called Denial-of-Service (DoS) attacks. This brute-force and technically simple cyberattack overloads an attacked server by flooding it with high levels of data traffic. Nevertheless, DoS attacks can cause high economic costs especially when they target bank and industry servers, suggesting that governments may use them for coercive purposes. Many pundits claim that cyberattacks are a new coercive tool for governments in international relations highlighting that the above stated example is not an exception (e.g., McLellan, 2018). While this view has been shared by one strand of the cyber conflict literature (e.g., Richard, Robert et al., 2010; Lynn III, 2010), previous theoretical works argue that cyberattacks are an ineffective instrument for coercion in international relations. After all, they are hard to attribute and deter, do not impose enough damage, and their effects are merely temporary (e.g., Gartzke, 2013; Rid, 2012; Nye Jr, 2017).

The goal of this paper is to empirically test these claims. I therefore explore whether the frequency of DoS attacks increases against countries that threaten or impose economic sanctions against other states. For this investigation I rely on a dataset of DoS attacks measured from Internet traffic between 2008 – 2016 containing information on the target of such attacks (CAIDA, 2016). As many cyber incidents happen covertly, this is one of the first studies shedding light on the use of DoS attacks using Internet traffic data. I focus on sanction periods because they can be perceived as a likely case, for which one could expect a digital response by the targeted state. This is because economic sanctions are one of the most aggressive foreign policies where targeted states have to respond with some action. Besides, previous literature largely neglected to investigate how states respond to sanctions. Cyberspace may have provided governments with new options to react through other channels (an exception is Cranmer, Heinrich and Desmarais, 2014).[1]

I propose two mechanisms why there might be an increase of DoS attacks on sending countries after the threat and/or imposition of sanctions. Firstly, following one strand of the literature, the targeted state employs DoS attacks as a coercive tool to create disruption costs in the sender state(s) and force them to concessions (coercion mechanism). Secondly, in an alternative mechanism, targeted states and/or groups within the country launch DoS attacks as a signal of discontent (contention mechanism). More precisely, I

[1] Although the in this paper developed theoretical considerations focus on sanctions, they may apply for other aggressive policy events as well, e.g., trade wars or kinetic conflict.

expect that the former mechanism should apply stronger when countries threaten sanctions because states can still avoid economic costs, and the latter when sanctions are imposed as elites and citizens are affected by sanctions and anti-sender sentiments are fueled. Furthermore, both effects should be more pronounced when the targeted state is technologically advanced.

In the empirical analysis, I run time series models to capture the short and long term effects of sanctions on DoS attacks against the United States (US) and the European Union (EU) on a daily level. The results show that sanction threats and impositions appear to be unrelated to the development of DoS attacks on sender countries. However, when I exclusively consider sanctions against technologically advanced countries, the results highlight a significant increase of DoS attacks on the United States when sanctions are imposed. While this points to some systematic pattern, further analyses show that this result is largely driven by a few cases only.

In conclusion, this study shows no systematic relationship between aggressive foreign policy events (i.e., sanctions) and DoS attacks. The results point even to an explicit null finding with regard to an increase of DoS attacks after sanction threats. Since it is more rational for governments to use DoS attacks as a coercive tool already when other states threaten sanctions, this finding adds doubts about whether governments use DoS attacks to gain concessions. An in-depth investigation of cyber events around the imposition of sanctions against Russia in 2014 supports this point. The case study suggests that it was not necessarily state actors that were directly behind DoS attacks, but more plausibly hacking groups and citizens voicing discontent via DoS attacks. Overall, this paper questions the use of DoS and other disruptive cyberattacks as an interstate warfare tool to gain concessions and may explain why previous literature could only find limited evidence for such a relationship (e.g., Valeriano, Jensen and Maness, 2018). In line with Gartzke (2013) and Rid (2012), the empirical findings suggest that cyberattacks appear to be an ineffective coercive instrument for governments.

4.2 Economic Sanctions and Digital Responses

There is a vast body of literature exploring economic sanctions and their consequences in political science. Following Pape (1997), economic sanctions are a coercive policy tool for a state A (or several states) to change unwanted policies or achieve institutional change in a target state B. While some studies show mixed results for the efficiency of sanctions (e.g., Pape, 1997; Marinov, 2005; Escribà-Folch and Wright, 2010), other scholars find a number of often unintended consequences for the targeted country. These include, increasing levels of anti-regime protests (Grauvogel, Licht and von Soest, 2017), increased government repression (Wood, 2008), worsening human rights conditions (Peksen, 2009) and, contrary to conventional wisdom, increased legitimacy for the government in power (Cortright et al., 2000; Grauvogel and Von Soest, 2014; Galtung, 1967).

Whereas most academic works have focused on the consequences of sanctions on the targeted country, less is known about the impact on the sender country and how targeted states react. The previous literature finds a negative impact of sanctions on trade flows (Caruso, 2003; Veebel and Markus, 2018), mixed evidence for government support in sender countries (Whang, 2011; Webb, 2018), and a higher likelihood of counter-sanctions as a response by the targeted country (Cranmer, Heinrich and Desmarais, 2014; Hedberg, 2018). More generally, targeted states have four options for how to respond to sanction threats and/or impositions. They can (1) change their behavior and policies, (2) refuse to change their behavior and bear the costs of the sanctions, (3) reach out to new trading partners to minimize costs, or (4) undertake active action to influence state A to not impose or lift sanctions (Cranmer, Heinrich and Desmarais, 2014). One way for the fourth option is the threat or imposition of economic counter-sanctions on state A (ibid.). However, states can also use other coercive means to reach this goal and increase state A's expected and actual costs of imposing or upholding sanctions.

The Internet has increased the available toolkit for states to try to change foreign policy behavior without reverting to brute force (Valeriano, Jensen and Maness, 2018). Valeriano, Jensen and Maness (2018) classify these cyber actions into three, potentially coercive, policy tools: disruption, espionage, and degradation. Digital disruption tactics include DoS and defacement campaigns, espionage the use of hacking and network intrusion and degradation describes large-scale cyber operations, the Stuxnet malware against Iran in 2010, for example. One of the first empirical studies on the topic finds that DoS attacks, in particular, are one of the most commonly used types of cyberattacks between adversary states (Valeriano and Maness, 2014). Further studies have mainly focused on the effect of cyberattacks, finding only limited support for an impact on (1) worsening interstate relations and (2) concessions by the targeted state (Maness and Valeriano, 2016; Valeriano, Jensen and Maness, 2018).[2] However, as systematic works on the drivers of cyberattacks are missing, this does not rule out that such tools are used to gain concessions. Another shortcoming has been the use of publicly available data by these studies. Relying on media-based data may lead to wrong conclusions on the use of cyberattacks because news outlets can report on public attacks only (cf. Poznansky and Perkoski, 2018). A notable exception is a recent study by Kostyuk and Zhukov (2019) that investigate the interplay between DoS attacks and battlefield events in Ukraine and Syria using data on DoS attacks by an Internet security company. They find no relationship between cyber and actual battlefield events.

In this paper, I propose that DoS attacks may be used as a digital response by countries targeted by economic sanctions due to two mechanisms. The first mechanism follows one strand of the previous cyber conflict literature and describes the process as a rational action by the targeted state to gain concessions (coercion mechanism). The second

[2]In fact, again the only type of cyberattack that is negatively correlated to interstate relations are DoS attacks (Maness and Valeriano, 2016).

mechanism offers an alternative explanation for why the targeted state launches DoS attacks and depicts the use of them as a contentious signal to protest against sanctions (contention mechanism).

Coercion mechanism: Comparable to economic counter-sanctions, targeted governments, either themselves or by ordering government-related hacking groups, may launch DoS attacks as a economically costly response to achieve concessions. DoS attacks can lead to severe economic costs for the attacked country. The cybersecurity firm Radware calculates that DoS attacks can cost up to several million dollars when they target banks or other economy relevant servers (Radware, 2019). Another cybersecurity firm speaks of costs around 40 000 US dollars per hour when a business website is put offline (Matthews, 2014). In fact, anecdotal evidence highlights that DoS attacks against US banks and energy companies in 2011–13 by presumably Iranian actors cost the companies several million dollars (Perlroth and Hardy, 2013).

Apart from economic costs caused by DoS attacks, a drastic rise of these attacks on servers within the sender state may also make a resolve signal by the targeted state to opt for more drastic responses more credible. Although DoS attacks are relatively brute-force and technically easy, a large-scale launching of DoS attacks should signal the sender that the targeted state possesses respective resources and higher levels of technological development.

An obvious requirement for this mechanism to work is that the sender state can attribute these attacks. However, particularly in the case of large-scale DoS attacks, it should be relatively clear for government agencies that increasing levels of DoS attacks against the sender country shortly after they threatened or imposed a sanction are related (cf. Valeriano, Jensen and Maness, 2018, p.31).

Finally, even though Valeriano, Jensen and Maness (2018) show in their empirical analysis that cyberattacks only rarely lead to concessions, their finding might underestimate the potential coercive impact of DoS attacks. This is because the empirical analysis of the authors only focuses on observable cyber activities, where states do not want to lose their face and thus may be less open for concessions.

Contention mechanism: The alternative mechanism describes the use of DoS attacks on the sender country as a contentious digital response by the targeted state. DoS attacks are launched against the sender state's government websites, news websites or nationally relevant servers, including industry and banks, thereby sending a signal of disapproval (cf. Lutscher et al., 2020).

Here, it might be not only targeted governments or government-related proxies that launch these attacks but citizens and hacking groups of the targeted state may also react on their agenda. The literature emphasizes that economic sanctions influence domestic behavior of citizens and may lead to the so-called "rally-around-the-flag effect" (e.g.,

Kaempfer, Lowenberg and Mertens, 2004). This meansthat sanctions may strongly reinforce nationalist sentiments of citizens and make them more susceptible to government propaganda (Cortright et al., 2000; Galtung, 1967; Haass, 1997), which even may encourage citizens to engage in collective action in favor of the government (cf. Hellmeier, 2019).

In an analysis of the use of DoS attacks during the Russo-Georgian war in 2008, Deibert, Rohozinski and Crete-Nishihata (2012) show that similar dynamics are likely to apply in cyberspace as well. The authors even argue that it was very plausible that it was Russian citizens, criminal groups and hackers alone that were responsible for the large-scale DoS attacks during the conflict. A similar conclusion is derived by Rid (2012), investigating the 2007 DoS attacks on Estonia. Nevertheless, these kind of DoS attacks are likely facilitated by the government of the targeted country due to their use of propaganda to take action against foreign aggression, as well as sponsoring of patriotic hacking groups.[3]

Observable Implications and Hypotheses What observable implications do these mechanisms have for the sender states?[4] In general, both mechanisms may explain an increase in the frequency of DoS attacks on the sender state(s) after the country/countries threatened or imposed sanctions. Thus, empirically we should expect that:

Hypothesis 4.1 *The frequency of DoS attacks rises against the sender state when it threatens sanctions.*

Hypothesis 4.2 *The frequency of DoS attacks rises against the sender state when it imposes sanctions.*

Although it remains difficult to clearly distinguish between the proposed mechanisms, I argue that the one or the other may more likely apply depending on whether the sender state threatens or imposes sanctions. From a rational viewpoint the coercive mechanism of DoS attacks should apply already more strongly when other states threaten sanctions. This is because the targeted state can still avoid economic costs completely if concessions are achieved. In contrast, the contention mechanism should apply more strongly when sanctions are imposed. First, elites and citizens are affected by the imposition of sanctions. Second, governments can use the imposition of sanctions to a greater extent to fuel negative sentiments against the sender state (cf. Galtung, 1967). Both points

[3]Since one can start DoS attacks globally, it has not to be only domestic citizens that may use these attacks. For example, the global collective *Anonymous* did not only started DoS attacks against the Qaddafi government in 2011, but factions within *Anonymous* used them in favor of the Qaddafi government (Partyvan, 2012).

[4]I focus on the implications for the sender countries because there is no systematic data of perpetrators of DoS attacks available that is not media-based. In addition to problems of media biases when using media-derived information on DoS attacks (see again in the research design section), information on the true perpetrator of cyberattacks derived from news reports is often not available and/or uncertain.

should make the voicing of discontent also by citizens and/or groups more likely when sanctions are imposed.

Thus, while both mechanisms may apply when sender states threaten or impose sanctions, a stronger increase after sanction threats would rather speak for the coercive function of DoS attacks. In contrast, a stronger rise of DoS attacks after the imposition of sanctions should more strongly support the contention mechanism. In the case of equal effects after threats and impositions it would remain unclear what mechanism to support.

Finally, country-specific characteristics of the targeted state influence the ability to launch digital responses. Although DoS attacks are rather easy to employ, states require a basic level of technological capabilities and resources to use DoS attacks at scale. Only these states can cause high disruptive costs by launching large-scale attacks, and their resolve signal to use advanced cyberattacks is more credible (Rid and Buchanan, 2015). In addition, citizens are more educated and technically sophisticated, making the existence of hacking groups and the use of more DoS attacks more likely. Thus, the final hypothesis is:

Hypothesis 4.3 *An increase in DoS attacks on the sender state after sanction threats or impositions is more likely observable when the targeted state is technologically advanced.*

4.3 Research Design

To investigate these hypotheses I create daily time series from 2008 – 2016 of DoS attacks against the most active sanctioning entities, the US and the EU. In the next subsection, I explain the DoS attack data in more detail, introduce the information on sanctions, as well as discuss how I measure technological advancement. Following this, I introduce the statistical model to analyze these time series.

4.3.1 Data

Dependent Variable In contrast to previous studies on interstate conflicts in cyberspace, I use a new dataset of DoS attacks collected by the Center for Advanced Internet Studies (CAIDA) at the University of California, San Diego from 2008 until 2016 (CAIDA, 2016). This data is one of the most comprehensive and fine-grained data sets on DoS attacks worldwide and comes with some major advantages compared to media-based approaches used in previous studies (e.g., Valeriano and Maness, 2014). CAIDA measures DoS attacks inferring them from Internet traffic and captures so-called "randomly spoofed" DoS attacks, where attackers craft their flood of requests to the target such that it appears to originate from one or several *fake* Internet addresses, i.e., not corresponding to the machine(s) executing the attack. 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 (Lutscher et al., 2020; Moore et al., 2006).[5] This measurement approach means that this data source is by construction not prone to media biases, neither media attention nor under-reporting of DoS attacks. Concerning the former, my approach avoids measurement errors because sanctions may increase not only DoS attacks but also the reporting of them as the sender and target state is in the center of attention. Regarding the latter, previous studies likely missed cyber incidents because many are not recorded in the media (Poznansky and Perkoski, 2018). The data by CAIDA can get a more comprehensive picture of DoS attacks as the data even contain the smallest attacks and attack attempts. Additionally, the data include information about attack strength and duration, the exact time of the attack, and the targeted IP address, which is used to infer the geographic location of the attacked server.

Nevertheless, the data come with some limitations (cf. Moore et al., 2006). First, CAIDA captures a subset of DoS attacks (randomly spoofed DoS attacks). Thus, the measurement can be described as a conservative approximation for the overall level of DoS attacks. Even so, recent studies show that spoofed DoS attacks are comparable in numbers to reflection attacks, which is another popular class of DoS attack vectors (see Jonker et al., 2017). Second, since attackers use fake addresses, I cannot infer the identity of the attacker or even the attack's country of origin. However, even if this information would be available, this often does not help as attackers use botnets, spoofing methods, and other techniques to hide their identities.

This paper focuses exclusively on the development of DoS attacks in the sender country/countries. For this, I retrieve the daily number of DoS attacks in the US and EU, summing up DoS attacks for each member state, from April 2008 until end of December 2015. Since the measurement failed in 6.9% of the observations and for most of the statistical analyses complete time series are needed, I use state-space models with a Kalman filter to fill up the missing values (Gardner, Harvey and Phillips, 1980). In Appendix E.2, I discuss this procedure in greater detail.

Explanatory variables To receive information about sanction threats and impositions, I rely on a recent dataset by Weber and Schneider (2019) that collects information about sanction periods from 1990 – 2016 for the US and EU as the most active country and supra-national entity imposing economic sanctions. I code the variable *sanction threat* as '1' for the beginning of each sanction period and the variable *sanction* is set to '1' at the imposition date ,if applicable. For the period of study, the data records 29 or 20 sanction threats and 28 or 23 impositions by the US or EU, respectively.[6]

[5] Approximately 1/256th of all IPv4 Internet addresses.

[6] In the few cases where the US or EU threatened or imposed more than one sanction at one specific date the variable remains binary. In five cases for the US, and two cases for the EU, sanction impositions and threats overlap on the same day, yet the targets are different.

To test Hypothesis 4.3, which expects that only technologically advanced countries respond digitally, I use data from the International Telecommunication Union (ITU) about a country's Information and Communication Technologies (ICT) development (ITU, 2017). Three clusters of indicators that measure the access to, use of and skills regarding modern ICTs create the so-called ICT Development Index (IDI). These clusters are then normalized and weighted to create an index ranging from 0 (no) to 10 (highest technological literacy). Since the ITU does not publish the IDI every year, I fill values for years in between using linear imputation. Then I use this information to create the variables *sanction threat (techno.)* and *sanction (techno.)* that only consider sanctions targeted on countries with IDI scores above 25% compared to the global year average. In later sensitivity test, I chose cut-off values of 50% and 75%.

Descriptive Overview Figure 4.1 shows the development of the main variables of interest from 2008 until 2016. The graph reveals some notable findings. First, the overall level of DoS attacks is much higher in the US compared to the EU. Second, there appears to be a similar trend between both time series. This trend may be primarily explained by the fact that most DoS attacks reflect criminal activities and servers of important services are hosted worldwide. Third, from approximately the year 2012 there is a sharp increase in the number of daily attacks for both time series. Potential reasons for this rise may be related to the increased use of cloud networks and DoS mitigation services, which make a higher attack frequency necessary, or simply more attacks.[7]

4.3.2 Method

To analyze the data, I use unrestricted Autoregressive Distributed Lagged (ARDL) models that can capture short- and long-term effects of variables of interest. ARDL models are parsimonious and widely used time-series models in economics and political science to investigate temporal relationships, allowing the inclusion of lagged independent and dependent variables (Hendry, 1995; Philips, 2018). Before I can run these models reliably and draw robust inference, my time series have to fulfill certain properties. The data should (1) have no structural breaks, (2) be stationary and (3) be normally distributed (cf. Baissa and Rainey, 2018). Since all these properties are initially not fulfilled, I split the time series (to solve problem 1), take first differences (problem 2) and transform these using a box-cox algorithm (problem 3). In Appendix E.3, I discuss these steps in greater detail. Finally, one has to decide on the maximal number of lags for the ARDL models. To keep the models parsimonious, I follow the literature and use the Akaike Information Criterion (AIC) to find the models with the best fitting lags (Burnham and Anderson, 2004; Pesaran, Shin and Smith, 2001).

I restrict the maximum number of lags the AIC selection algorithm can choose to

[7] As confirmed by CAIDA, the increase of attacks is not due to a change in the measurement procedure.

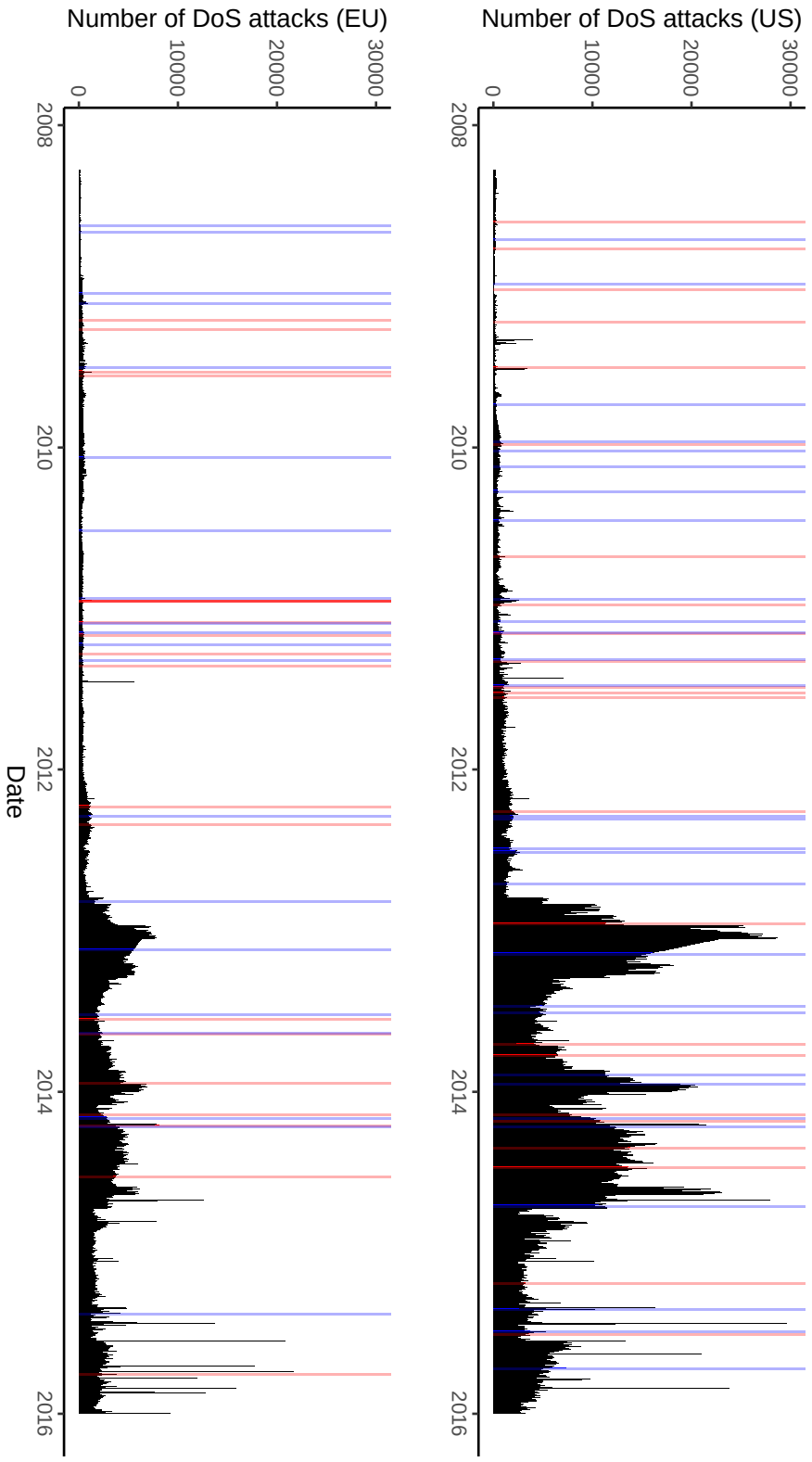

Figure 4.1: DoS attacks on the US/EU and sanction periods (2008 – 2016). Note: Development of DoS Attacks (grey), sanction impositions (red) and sanction threats (blue). Note: Outliers with values above 30000 attacks per day are not shown.

14 days because a digital response to sanction threats and impositions should happen relatively soon afterward.[8] The model can be summarized as follows:

$$\Delta DoS_t = \alpha_0 + \sum_{i=1}^{p} \alpha_i \Delta DoS_{t-i} + \sum_{j=0}^{q} \beta_j sanction_{t-j} + \sum_{k=0}^{r} \beta_k threat_{t-k} + \epsilon_t \tag{4.1}$$

where p is the maximal number of lags for the dependent variable, q for the sanction imposition variable and r for the sanction threat variable.

4.4 Results

In the following, I report the main results of statistical analyses, several robustness and sensitivity tests and discuss whether we see a systematic increase of DoS attacks after sanction threats or impositions.

4.4.1 Main models

Table 4.1 shows the main regression results that allow to evaluate the direction of an estimate and whether a variable has a time effect. At first glance, it appears that the coefficients of the sanction imposition variable are mostly positive, while the opposite is true for sanction threats. Besides, for the sanction imposition variable the models suggest the inclusion of temporal lags, while for the threat variable this is not the case.

One common way for ARDL models to investigate temporal effects of variables is to calculate the so-called long-run multiplier (LRM) coefficient (Wooldridge, 2015). This statistic is the temporally aggregated coefficient of the variable of interest, i.e. the overall effect size, and allows to not only investigate the direction but also the magnitude of a variable's impact. The following equation shows how this multiplier is calculated:

$$LRM = \frac{\sum_{i=0}^{p} b_i}{1 - \sum_{j=1}^{q} a_j} \tag{4.2}$$

Table 4.2 reports the LRM coefficient for the sanction imposition variable for all eight models. For the US time series, all coefficients are positive. The time series greater than 2012-02-13, which considers sanctions against technologically advanced countries, highlights the largest coefficient. The coefficients for the EU are also mostly positive (but considerably smaller) and display higher values when considering sanctions against more technological countries. These results support a positive association between the imposition of sanctions and a rise in the number of DoS attacks, in particular when

[8] I expand this period in later robustness tests. Furthermore, I include more lags of the dependent variable when the model still shows problems with autocorrelation. Using the Bayesian Information Criterion (BIC) for the model selection leads to much fewer lags. Since the goal of this study is to determine whether sanctions are at all correlated to DoS attacks, I use the AIC.

	Δ DoS US <= 2012-02-13	Δ DoS US > 2012-02-13	Δ DoS US <= 2012-02-13 (techno.)	Δ DoS US > 2012-02-13 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction	0.14	0.38	0.34	0.09	0.53	0.67	0.75	1.31
	(0.39)	(0.45)	(0.66)	(0.66)	(0.36)	(0.55)	(0.53)	(0.73)
Sanction (t-1)	−0.07			−0.55	0.41			0.56
	(0.39)			(0.66)	(0.35)			(0.74)
Sanction (t-2)	0.21			0.44	0.12			−1.27
	(0.39)			(0.66)	(0.35)			(0.74)
Sanction (t-3)	0.69			−0.03	0.58			−0.11
	(0.39)			(0.66)	(0.35)			(0.74)
Sanction (t-4)	1.04**			0.79	−0.54			−1.42
	(0.39)			(0.66)	(0.35)			(0.74)
Sanction (t-5)				0.56	−0.72*			1.97**
				(0.66)	(0.35)			(0.74)
Sanction (t-6)				−0.03	−0.66			
				(0.66)	(0.35)			
Sanction (t-7)				1.53*				
				(0.66)				
Sanction (t-8)				1.18				
				(0.67)				
Sanction (t-9)				0.31				
				(0.67)				
Sanction (t-10)				2.07**				
				(0.67)				
Sanction (t-11)				1.23				
				(0.67)				
Sanction (t-12)				−0.36				
				(0.67)				
Sanction (t-13)				0.07				
				(0.67)				
Sanction (t-14)				0.69				
				(0.66)				
Sanction threat	−0.22	−0.43	−0.01	−0.26	0.42	−0.87	−0.11	−0.11
	(0.41)	(0.42)	(0.49)	(0.58)	(0.34)	(0.58)	(0.48)	(0.73)
Sanction threat (t-1)			−0.77					
			(0.49)					
Δ DoS (t-1)	−0.27***	−0.21***	−0.26***	−0.21***	−0.41***	−0.38***	−0.40***	−0.38***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.21***	−0.16***	−0.21***	−0.16***	−0.34***	−0.22***	−0.33***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.18***	−0.16***	−0.18***	−0.16***	−0.22***	−0.21***	−0.22***	−0.21***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.09**	−0.00	−0.09**		−0.22***	−0.09**	−0.23***	−0.09**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-5)	−0.05	−0.05	−0.05		−0.15***	−0.09**	−0.16***	−0.08**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-6)	−0.07*	−0.01	−0.08*		−0.11***	−0.10**	−0.11***	−0.10**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-7)	0.00	−0.00	0.00		−0.09**	−0.03	−0.09**	−0.04
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-8)	−0.02	−0.00	−0.02		−0.06*	−0.00	−0.06	−0.00
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-9)	0.00	0.06*	0.01		−0.08*	−0.03	−0.07*	−0.04
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-10)	0.02	0.01	0.02		−0.06*	−0.01	−0.06*	−0.01
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-11)	−0.06	0.05	−0.05		−0.10**	−0.04	−0.10**	−0.04
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-12)	−0.05	0.01	−0.04		−0.08*	−0.03	−0.08*	−0.03
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-13)	−0.02	−0.01	−0.02		−0.02	0.02	−0.02	0.02
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-14)	0.05*	0.07*	0.06*		−0.01	0.07**	−0.00	0.07**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
R^2	0.11	0.08	0.10	0.08	0.18	0.16	0.17	0.16
Adj. R^2	0.10	0.07	0.09	0.07	0.17	0.14	0.16	0.15
Num. obs.	1388	1402	1388	1402	1375	1415	1375	1415
RMSE	1.46	1.63	1.46	1.62	1.16	1.64	1.16	1.64

Table 4.1: Main Autoregressive Distributed Lagged (ARDL) models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

the United States imposes sanctions against technologically advanced countries. However with the LRM coefficient it is hard to determine the levels of uncertainty for this relationship.

Variable	Long-run multiplier coefficient
Sanction US <= 2012-02-13	1.04
Sanction US > 2012-02-13	0.27
Sanction US (techno.) <= 2012-02-13	0.18
Sanction US (techno.) > 2012-02-13	5.19
Sanction EU <= 2012-01-31	-0.09
Sanction EU > 2012-01-31	0.31
Sanction EU (techno.) <= 2012-01-31	0.25
Sanction EU (techno.) > 2012-01-31	0.49

Table 4.2: Long-run multiplier coefficients.

To gain an understanding of the uncertainty around these results, newer approaches suggest running simulations of the models to investigate counter-factual cases for variables of interest (Philips, 2018). To run these simulations, I set the sanction threat variable to 0 and the imposition variable to 1. Furthermore, I set the intervention to the point in time 5 (dashed vertical line), and the dashed horizontal line represents the untransformed ΔDoS value of 0 (null effect).

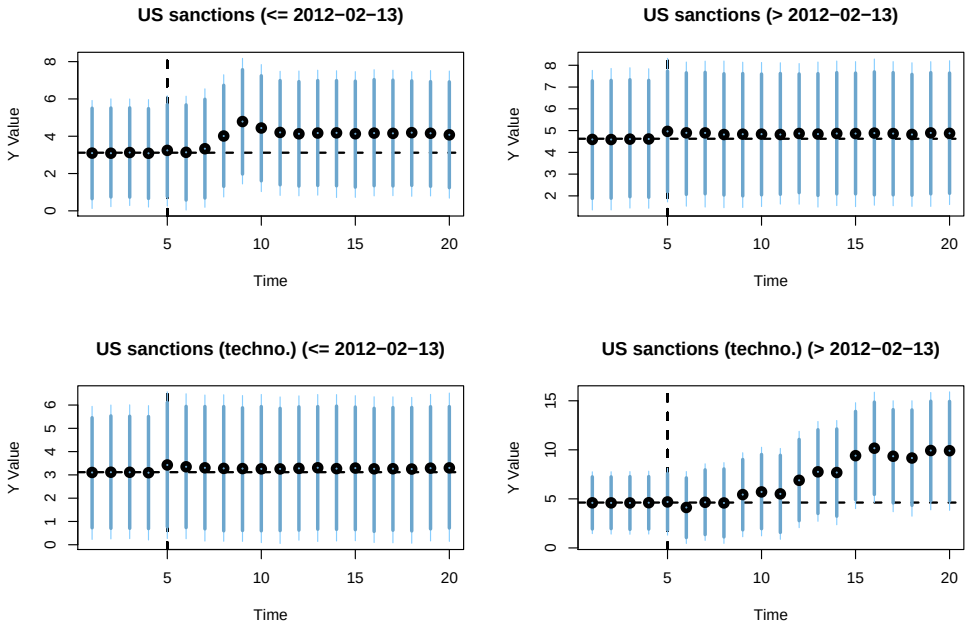

Figure 4.2: Simulations of DoS attacks (US). Note: Based on 10000 draws. 95% and 90% confidence intervals are displayed.

Most simulations highlight small, if any, increases of DoS attacks beyond conventional levels of significance. However, for the US time series greater than 2012-02-13 that

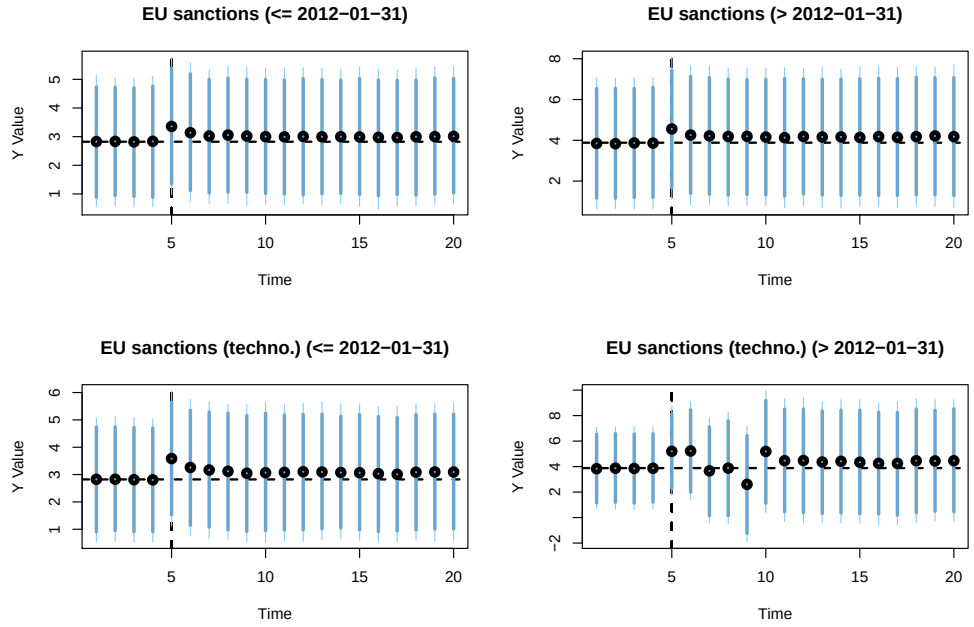

Figure 4.3: Simulations of DoS Attacks (EU).

considers sanctions against technologically advanced countries, the simulation shows a systematic and significant pattern. For this time series we see a steady increase of DoS attacks, with a peak at day 11 after the imposition date, where the simulated value is distinguishable from the horizontal dashed line (null effect).[9] From this, one can conclude that sanctions *per se* are not systematically related to an increase of DoS attacks on the sender country but we do see some systematic pattern when it comes to sanctions against more technologically developed countries.

One concern might be that the analysis faces problems of reverse causality. In fact, the United States imposed sanctions against Iranian citizens recently because they were alleged to be involved in the large-scale DoS attacks against the US between 2011 and 2013 (Volz, 2018). While this example emphasizes that it is rather unlikely that governments impose sanctions directly after a cyberattack hit the sender country, it might be that targeted countries already launch DoS attacks before the imposition date. To test whether this is the case I run Granger (causality) tests, showing whether the inclusion of lags increase the model fit (F statistic) for the respective models, where the dependent variable is either ΔDoS or *sanction*.

Table 4.3 shows that in the case of the US time series, two models with DoS attacks as dependent variable display a significantly better model fit. This finding supports the previous results and highlights that sanctions do explain some variance in the development

[9] While these simulations allow to draw robust statistical inference, the untransformed predictions are imprecise, predicting an increase of 36,943 DoS attacks. In later robustness tests, I additionally run untransformed models that show similar patterns predicting an increase of approx. 5000 attacks (see Figure E.4.6).

F	Pr(>F)	Direction	Country	Time
2.53	**0.04**	**Sanction -> DoS**	**US**	**<= 2012-02-13**
0.87	0.59	DoS -> Sanction	US	<= 2012-02-13
No lag	No lag	Sanction -> DoS	US	> 2012-02-13
0.72	0.75	DoS -> Sanction	US	> 2012-02-13
No lag	No lag	Sanction (techn.) -> DoS	US	<= 2012-02-13
0.55	0.91	DoS -> Sanction (techn.)	US	<= 2012-02-13
1.76	**0.04**	**Sanction (techn.) -> DoS**	**US**	**> 2012-02-13**
0.25	0.86	DoS -> Sanction (techn.)	US	> 2012-02-13
2.45	**0.02**	**Sanction -> DoS**	**EU**	**<= 2012-01-31**
1.97	**0.02**	**DoS -> Sanction**	**EU**	**<= 2012-01-31**
No lag	No lag	Sanction -> DoS	EU	> 2012-01-31
0.89	0.57	DoS -> Sanction	EU	> 2012-01-31
No lag	No lag	Sanction (techn.) -> DoS	EU	<= 2012-01-31
2.01	**0.01**	**DoS -> Sanction (techn.)**	**EU**	**<= 2012-01-31**
3.04	**0.01**	**Sanction (techn.) -> DoS**	**EU**	**> 2012-01-31**
0.44	0.96	DoS -> Sanction (techn.)	EU	> 2012-01-31

Table 4.3: Granger tests. Bold highlighted directions are significant at $p < 0.05$. The number of lags is used from the previous models.

of DoS attacks. While for some EU time series this is the case as well, here the Granger tests also highlight that DoS attacks correlate to sanctions before their imposition for the less than or equal to 2012-01-31 time series.

In conclusion, the empirical analysis finds the following. First, the results do not support Hypothesis 4.1 that expects an increase of DoS attacks on the sender country after the country threatened sanctions.[10] Second, the analysis does not clearly support Hypothesis 4.2 that expect an increase of DoS on the sender country when sanctions are imposed. However, when I exclusively consider sanction impositions against technologically advanced countries (Hypothesis 4.3), the results show some systematic pattern with regard to an increase of DoS attacks on the United States.

Regarding the theoretical mechanisms, these results challenge the coercive use of DoS attacks to gain concessions. This is because from a rational view it makes for the targeted state more sense to already influence a sender's behavior before the imposition of sanctions to avoid costs completely. By deduction this means that the systematic increase of DoS attacks on the US after they impose sanctions on technologically advanced countries is more likely a contentious response by the targeted country.

[10] A concern may be that the inclusion of both variables biases inference for the sanction threat variable because the imposition of sanctions can be considered as a "post-treatment" variable. Running similar analyses with the sanction threat variable alone also suggest a null finding of sanction threats (see Figures E.1.1 – E.1.2 and Table E.1.1). Another shortcoming is that it may be that within the sanction periods the sender state(s) reinforced threats and impositions gradually that may cause digital responses. Information that is unfortunately not available in Weber and Schneider (2019).

4.4.2 Robustness and Sensitivity Tests

To see how valid this conclusion is, I conduct several robustness and sensitivity tests that are reported in Appendix E.4 in greater detail.

1. I employ different thresholds to define technologically advanced countries, considering sanctions on countries with an ITU score above 50% or 75% of the worldwide year average. Due to fewer sanction cases, these analyses are restricted to the time series greater than 2012-02-13 (US) and 2012-01-31 (EU), respectively. The results show a stronger increase, the higher the technological development of countries targeted by sanctions (see Figures E.4.1).

2. It may be that the found relationship is not specific for DoS attacks on the US but captures a global trend. To test this, I conduct a placebo test using the number of worldwide DoS attacks as the dependent variable. The results do not show the same relationships anymore confirming that the development is US-specific (see Figure E.4.2 and Table E.4.2).[11]

3. It is not the technological capability of the target country that is important but other country features. To test this, I conduct placebo tests considering sanctions against countries with a logged GDP p.c. above 25% of the worldwide year average (World Bank, 2019). The found patterns are very similar, suggesting that not necessarily a country's technological advancement but general economic development is important (see Figure E.4.3 and Table E.4.3).[12]

4. Since the DoS data captures even the smallest attacks that may simply be noise, I only consider large DoS attacks, defined as belonging to the top 30% of attacks on a country/year as measured by the intensity of the data traffic used in the attack. The patterns remain the same and are additionally near to borderline significance for the first US and second EU time series when technologically advanced countries are targeted (see Figure E.4.4–E.4.5 and Table E.4.4).

5. It may be that the chosen lag length is too short. When I extend the maximal lag length to 21 days, the number of optimal lags remains the same for the independent variables (see Table E.4.8).

6. Running models without using the box-cox transformations highlight similar results and even show a significant increase for the lesser than or equal to 2012–02–13 US time series on technologically advanced countries (see Figures E.4.6–E.4.7 and Table E.4.5).

[11] Only for the time series smaller than or equal to 2012–01–17, which focuses on technologically advanced targets, a slight non-significant increase is observable.

[12] In fact, the two variables highly correlate with r = 0.9, making it difficult to distinguish both concepts.

7. Comparing the regression tables when I run the models without NA imputations shows the same patterns as in the main models (see Table E.4.6).[13]

8. When I aggregate the models to a one-week granularity this leads to higher levels of uncertainty but still similar patterns (see Table E.4.7 and Figures E.4.8–E.4.9).

Overall, these additional models support the main finding that US sanction impositions against technologically advanced countries increase the frequency of DoS attacks against servers within the US. Nevertheless, a final test that distinguishes between different sanction types adds doubt on how systematic this pattern is.

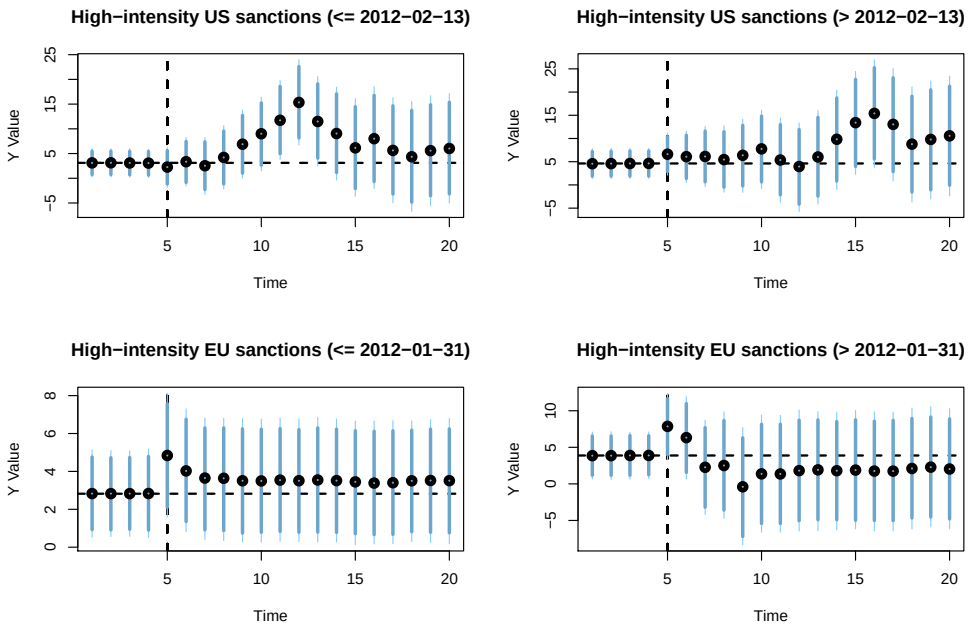

Figure 4.4: Simulations of DoS Attacks (US & EU) - High-intensity sanctions.

For this test, I discriminate between targeted (asset freezes, travel bans), low-intensity (import/export restrictions, termination of foreign aid, suspension of economic agreements, diplomatic sanctions) and high-intensity sanctions (economic embargoes, blockades, major financial sanctions).[14] Inspecting the sanctioning types reveals that targeted sanctions are related to an increase of DoS attacks for the US time series greater than 2012–02–13, again stronger, considering sanctions on technologically advanced countries (see Figure E.4.10). Furthermore, Figure E.4.12 highlights that low-intensity sanctions are positively related to an increase of DoS attacks in the US time series smaller than or equal to 2012–02–13. While this suggests no apparent pattern, the most substantial increase is observable when one considers high-intensity sanctions only. Figure 4.4 highlights a significant rise of DoS attacks in both US time series and even in one of the EU

[13] Due to the NAs simulations were unfortunately not possible.

[14] Since sanction types are often combined, this categorization is not exclusive. Another caveat is that this information is coded ex-post and aggregated for the whole sanctioning periods.

time series. In the period of study, the EU and the US imposed only two high-intensity sanctions. For the first period, these were sanctions against Syria in 2011 and for the second period, sanctions against Russia starting in March 2014. These findings suggest that these cases, and in particular the latter, are the main drivers of the statistical analysis. Thus, a systematic relationship between sanctions and DoS attacks remains limited.[15]

4.5 The Crimean Crisis in 2014

The statistical results show the most substantial increase of DoS attacks for the US time series greater than 2012–02–13. As shown, this result appears to be primarily driven by sanctions against Russia in 2014, making it worthwhile to investigate this case in greater detail.

After the Russian invasion of the Crimean peninsula on February 27, 2014, Western states condemned this action as illegal and threatened with consequences if Russia would not withdraw their troops. Because the Russian authorities did not comply, the United States imposed first sanctions on March 6, which included travel bans and the freezing of US assets for some Russian officials. Again, instead of complying, the Russian authorities announced an "independence" referendum of the Crimean peninsula on March 16 and the Russo-Ukraine conflict escalated. On March 15, the United States started an initiative in the Security Council that should condemn the Russian aggression as well as reinforced sanctions on March 17 after the referendum took place. The European Union undertook similar actions and imposed visa restrictions and froze assets. Nevertheless, on March 18, Russia annexed the Crimean peninsula. In addition, the countries Canada, Australia, New Zealand, and Japan imposed sanctions against Russia around the same dates.

Figure 4.5 shows the development of DoS attacks in the US and EU. The top panel reveals that attacks on the US peaked 11 days after the US imposed their first set of sanctions, explaining the spike in the main models after 11 days. It appears that the spike is related to the reinforcement of sanctions and the increased tension during the referendum weekend (March 15 – 17). Similarly, the same rise is visible in the frequency of DoS attacks against the European Union with the highest increase on the imposition date (bottom panel). Focusing on the other sanctioning countries lend support to this finding (see Figure 4.6). In particular, the number of DoS attacks on Canada increased drastically when the country imposed sanctions and for Australia when they supported the Security Council resolution by the US. Furthermore, Figure E.1.3 in the Appendix illustrates that DoS attacks on Russia and Ukraine spiked during the same periods showing a digital clash between both nations.

What can be said about the potential perpetrators and motivations in this case? First,

[15] In fact, running models without considering sanctions on Russia in 2014 still shows similar patterns, however, the results miss conventional levels of significance (see Figure E.4.14 and Table E.4.12).

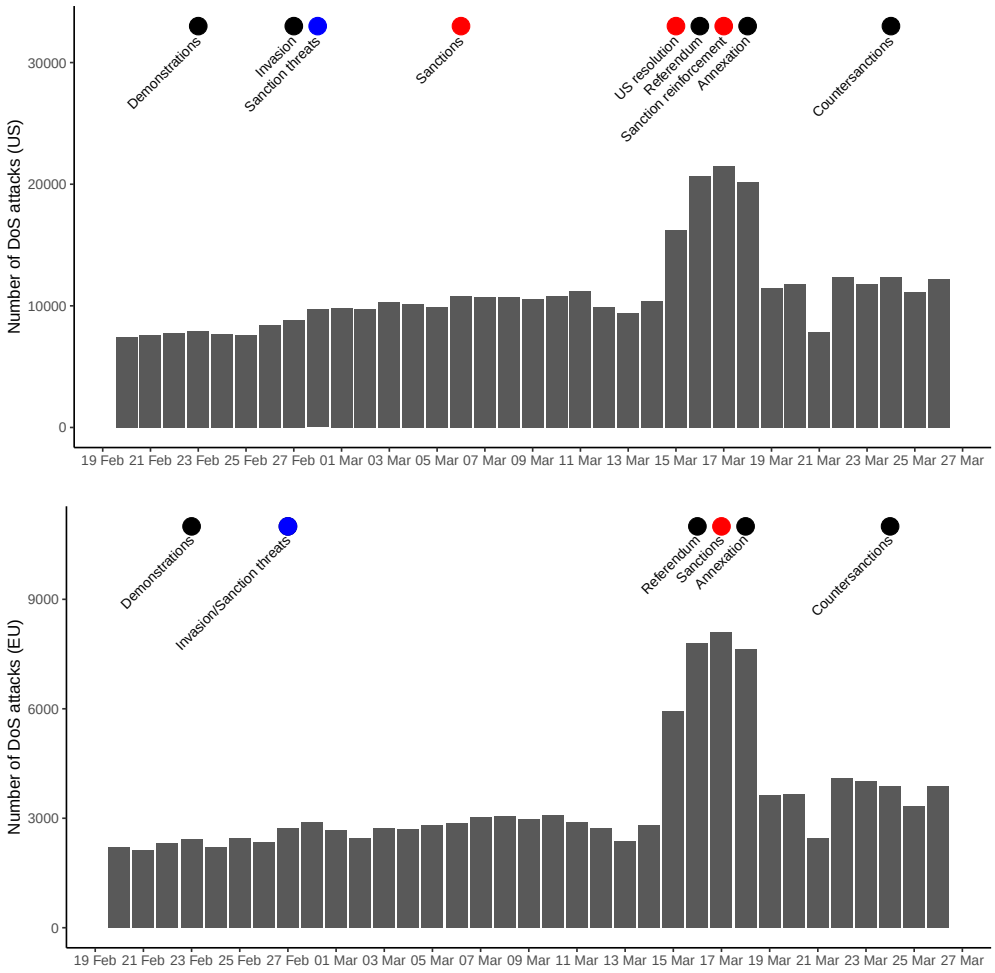

Figure 4.5: Number of DoS attacks in the US & the EU (February/March 2014). Note: Development of DoS Attacks (vertical bars), sanction related events (red dots), threats (blue dots) and other events (black dots).

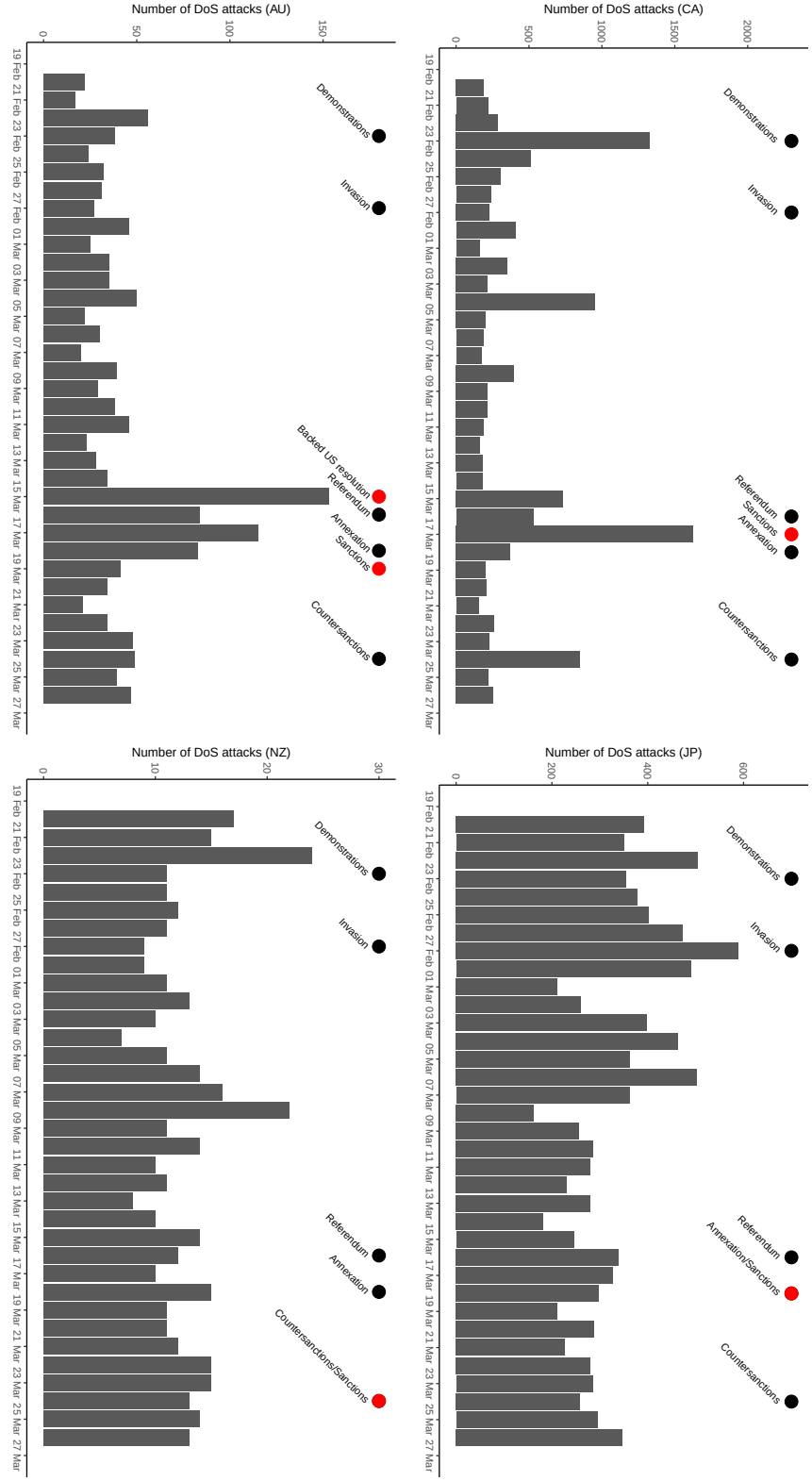

Figure 4.6: Other sanctioning states (February/March 2014).

botnet activities originating from Russia and the Ukraine spiked during this period, suggesting that Russian botnets were used to launch DoS attacks (Gilbert, 2019). Second, news outlets reported about DoS attacks against NATO websites on March 16 and the Estonian Foreign Ministry on March 19 by a group named Cyber Berkut. This group emerged in 2014 as a Ukrainian pro-Russian hacktivist group with an anti-Western stance (Cherney, 2014). Third, a Google trend investigation of the term "Denial-of-Service attack" in Russia shows considerable correlations with the US and EU time series (r=0.56 and r=0.51, respectively). The trend measures the interest for a search term, where interest is defined as the share of the search term to the absolute search volume for a given day, relative to the highest search volume for the period of study. Figure 4.7 shows that the trend gained momentum after the imposition of the US sanctions and especially just before the referendum weekend. Looking at geographical patterns illustrates that users in regions close to the Ukraine did search more often for DoS attacks. Besides, the Russian Google trend for "Low Orbit Ion Cannon", which is an easy to use tool for activists to conduct DoS attacks, highlights similar patterns.[16] Although the involvement of government entities cannot be excluded, the presented evidence rather supports the use of DoS attacks as a mean to show discontent by patriotic hacking groups and citizens (cf. Deibert, Rohozinski and Crete-Nishihata, 2012). Besides, the rather short duration also speaks more likely for a contentious response of these attacks.[17]

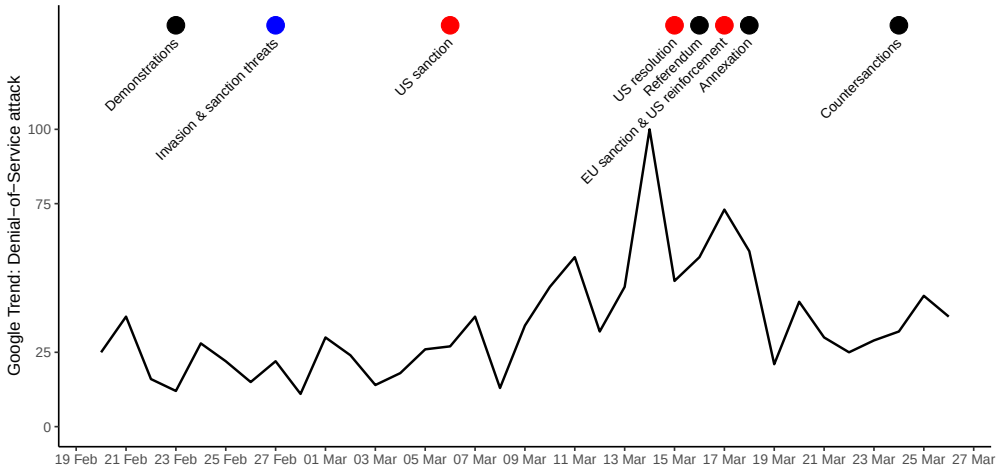

Figure 4.7: Russian Google Trend for DoS attack (February/March 2014).

An alternative explanation for the shown increase is that perpetrators did not launch DoS attacks against US or EU government-related servers but against servers that host Ukrainian websites in the US or EU (cf. Lutscher et al., 2020). Although this was certainly also the case, the increasing number of DoS attacks on other sanctioning countries

[16] Due to the specificity, this term is more volatile, making it challenging to investigate systematically.

[17] Similar reasons may explain the increasing level of DoS attacks after the imposition of sanctions against Syria in 2011, where it is likely that the patriotic hacker group "Syrian Electronic Army" was involved (Fisher and Keller, 2011).

and the presented anecdotal evidence support the conclusion that US and EU related servers suffered from DoS attacks in this case as well.

4.6 Conclusion

Using Internet traffic data to measure DoS attacks, this study finds only limited evidence for an increase of these attacks after sanction threats and impositions. Concerning the former, the results suggest a null finding, while DoS attacks rise after the imposition of sanctions in only a few cases. On the one hand, this result is surprising as sanction periods appear to be among the most likely cases where one should expect the use of cyber tools as digital response. This expectation appears to be even truer when focusing on the use of DoS attacks as a relatively simple but disruptive attacking tool.

On the other hand, the empirical results support previous studies that argue that cyber tactics play only a limited role in the foreign policy toolkit of states and that they are an ineffective coercive instrument (Rid, 2012; Gartzke, 2013). It seems that in the most cases the timing of DoS attacks is unrelated to aggressive foreign policy events. Besides, due to the attribution problem of cyberattacks and false-flag campaigns, it remains difficult to pinpoint the perpetrators of these attacks. In the few cases where the analysis could find empirical support for an increase of DoS attacks after sanction impositions, qualitative evidence suggests that there was likely no coercive logic behind their use but rather that hacking groups and citizen launched DoS attacks out of patriotic sentiments as a contentious response. This conclusion does not mean that state actors do not employ cyberattacks. In fact, governments likely sponsor patriotic hacking groups and facilitate their actions, as well as launch own espionage and infiltration campaigns. However, the results of this paper provide evidence for a non-coercive use of DoS and likely other cyberattacks.

5 Conclusion

In the last decades, humankind experienced one of the fastest technological revolutions. Modern ICTs, predominantly the Internet, changed how we gather information and communicate. This development has influenced economic, social, and political processes profoundly. At the same time, however, the growing interconnectedness of today's world and dependence on the Internet made this global network also more vulnerable. In this dissertation, I have illustrated how cyberattacks, more precisely DoS attacks, target servers worldwide and are used for political purposes in and by authoritarian countries. In contrast to most of the previous literature, I have not only focused on the international dimension of DoS attacks but explored the domestic reasons why activists and governments or government-related groups use DoS attacks in autocracies. In the remaining part of this chapter, I discuss the main contributions and findings of my dissertation, their meaning for the study of digital politics, derive some important policy advise and outline avenues for future research.

5.1 Contributions

There are three main contributions of my dissertation. First, I connect literature from the social movements, autocratic politics, and international relations fields of study. Second, I propose two parsimonious theoretical explanations for the main political uses of DoS attacks in autocracies. Third, I use two new measurements of DoS attacks from Internet data traffic and websites queries and combine them with political events and other data to test my theoretical expectations empirically. Generally, my studies

contribute to our understanding of digital politics and suggest that the censoring use of political DoS attacks in autocracies appears to be the most pronounced.

5.1.1 A Unified Theoretical Framework

Thus far, research in political science and sociology has separately investigated the different political aspects of DoS attacks. Firstly, the social movement literature has focused on the use of DoS attacks as a protest tool by hacktivist groups. Secondly, the international relations literature has investigated the use of DoS attacks in state-led cyber campaigns or cyberwar. Thirdly, the literature on authoritarian politics has pointed to the potential use of DoS attacks as a censoring tool for authoritarian governments. In this dissertation, I connect scholarly work from all three fields to gain a more holistic understanding of the political use of DoS attacks in autocracies. In a nutshell, I argue that the main political uses of DoS attacks in authoritarian regimes are to censor and contend.

On the one hand, authoritarian governments or government-related groups use DoS attacks as a means to censor threatening websites and content. DoS attacks are a convenient tool for this task because they are quickly mounted, can target servers/websites globally, are technically easy, and it is hard to trace them back. In the case of successful attacks, DoS attacks disable complete websites making it at least temporally impossible to access the attacked website for users worldwide. This outcome of a DoS attack speaks primarily for a what I call just-in-time censorship use of DoS attacks. The goal of this mechanism is to hinder the spread of threatening information exactly then when it is needed. However, throughout my dissertation, I also emphasize that DoS attacks have a repressive function. By this, I mean that governments or government-related groups launch DoS attacks as a tool to punish outlets and organizations. The goal of this mechanism is to send the attacked websites a repressive signal and change their behavior in their future, foster self-censoring, for example.

On the other hand, I propose that DoS attacks in autocracies are also commonly used as a tool for contention. Following this logic, activists, groups or other entities launch DoS attacks against specific targets to protest and signal discontent. Since DoS attacks are hard to trace back, they are a low-cost and relatively safe tool to state dissatisfaction in authoritarian governments, where normal channels of contention are often very costly. Whereas activists and opposition groups may launch these attacks against government and government-related websites to protest against government actions or policies (e.g., electoral fraud), also pro-government groups or government entities may use DoS attacks against foreign states to signal their displeasure with regard to foreign government's policies or actions, the imposition of sanctions, for instance.

5.1.2 A Systematic Empirical Analysis

In general, there have been only a few studies on politically motivated DoS attacks. Most of the previous studies, especially from the social movement and authoritarian politics fields, consist of case studies and anecdotal evidence only. While more empirical work has been done concerning the international dimension of cyberattacks (e.g., Valeriano, Jensen and Maness, 2018), most of these studies are temporally highly aggregated and rely on media sources to code politically motivated DoS attacks.

The use of media-derived data comes with problems of media biases that may lead to measurement errors. First, only public DoS attacks are reported (Hardy et al., 2014; Poznansky and Perkoski, 2018). Second, news agencies are driven by the newsworthiness of events, meaning that outlets report more likely about spectacular and bigger DoS attacks (cf. Earl et al., 2004). Third, theoretical concepts of interest may be related to the reporting of DoS attacks and determine whether DoS attacks occur or not (cf. King, Keohane and Verba, 1994). Finally, news outlets tend to report on countries that are of global interest or share the language of the newspaper.

The approach of my dissertation is different and I use two different data sources and measurements of DoS attacks that are independent of media sources and temporally disaggregated. The first comes from a collaboration with CAIDA providing data on randomly spoofed DoS attacks on a fine-grained temporal resolution for all countries worldwide from 2008 (CAIDA, 2016). The second is created from an own measurement of news websites in several autocracies from November 2017 until June 2018. For this measurement, I set up a server that contacted the news websites continuously and retrieved their status code, checking whether they are reachable or not. With both data sources, I can investigate DoS attacks on a worldwide macro level over time as well as on a micro level having specific information on the targeted website.

More precisely, in the first study (Chapter 2), I examine the question of whether DoS attacks increase during election periods worldwide from 2008 until 2016 using the data provided by CAIDA. In the second study (Chapter 3), I use my measurement approach to investigate the relationship between news content and DoS attacks on a newspaper/day level in Venezuela. In the third study (Chapter 4), I again use the data provided by CAIDA, this time daily times series for DoS attacks on the United States and European Union from 2008 until 2016.

Although there remain shortcomings of the approach taken in this dissertation, I can draw a more comprehensive and potentially less biased picture of the use of DoS attacks compared to previous literature that relied on media-based data. One main limitation of my approach is that I am only able to analyze the victims of DoS attacks. However, empirical analyses that use media-derived data can also not adequately solve this so-called attribution problem of cyberattacks, that is, the challenge to determine the true perpetrators of these attacks.

5.1.3 Implications for the Study of Digital Politics

In the following, I summarize the results of my studies and highlight the papers' implications for the study of digital politics. In discussing these implications, I order the discussion along the three distinct fields of study as well as their relevance for these fields: authoritarian politics, international relations, and social movements.

Authoritarian Politics Most importantly, this dissertation contributes to our understanding of how authoritarian governments use new technologies to censor and repress even beyond their borders. Previous literature exploring this use of cyber and DoS attacks only consisted of case studies and anecdotal evidence, making it difficult to evaluate how widely DoS attacks are used for this purpose. The results of the first study (Chapter 2) highlight that the frequency of DoS attacks against servers in countries that host news websites of authoritarian countries (foreign hosts) increases during election periods in the respective autocracy. This result suggests a systematic censoring use of DoS attacks by presumably authoritarian governments and/or government-related groups during sensitive times. The second paper (Chapter 3), in which I investigate DoS attacks on news websites, supports this finding. Here, I find a considerable number of DoS attacks against news websites from November 2017 until June 2018 in Venezuela.

Furthermore, the second paper (Chapter 3) does not only contribute to our understanding of why and when DoS attacks are used against outlets but also advances the literature on censorship and information control in authoritarian regimes more broadly. In this study, I test whether the censoring use of DoS attacks is to silence threatening websites and content just-in-time or if governments or government-related groups use these attacks to punish news outlet for actual and previous reporting on unwanted issues. Overall, the results show a more pronounced use of DoS attacks as a repressive tool. Whereas authoritarian governments also use physical means of repression against journalists and organizations to achieve this (cf. Frantz and Kendall-Taylor, 2014), cyberattacks enable autocracies to export censorship and repression abroad because they can easily target individuals and organizations worldwide. Besides, the finding of a differentiated censorship use of DoS attacks may likely travel to other forms censorship. For example, temporary blocking of websites by other technical means may not be only used to censor content just-in-time but rather to send repressive signals to the censored outlet potentially leading to behavioral changes in the targeted organization.

Nevertheless, the results of my studies also raise some doubts on (1) how widely DoS attacks are used for censoring purposes and (2) how effective DoS attacks are in that regard. In the first paper (Chapter 2), our statistical analysis finds a maximal increase of approximately 15% of DoS attacks during election periods in highly authoritarian regimes. In absolute terms, this means that, if the baseline of DoS attacks on a country is 100 DoS attacks, 15 additional attacks would be launched due to censoring purposes.

In general, this does not appear too high and emphasizes that most DoS attacks are unpolitical. Furthermore, questioning the effectiveness of DoS attacks, the descriptive statistics in the second paper (Chapter 3) show that the majority of the measured DoS attacks on newspapers are very short. Besides, additional models that investigate whether news websites change their reporting behavior after DoS attacks find only limited evidence for a change. Apart from the short duration of most DoS attacks, an explanation for this finding may be that many websites protect themselves by using DoS mitigation services. In conclusion, these points question how effective DoS attacks are as a censoring tool for authoritarian governments. Other techniques such as online filters on the Internet Service Provider (ISP) level may prove to be a more efficient way for authoritarian governments to censor the Internet, although users can more easily circumvent them. However, to conclude this in a informed manner, future research should investigate the consequences and effectiveness of DoS attacks as a censoring tool more closely.

International Relations Concerning the international use of DoS attacks, my dissertation helps to gain a better understanding of the use of cyberattacks in international relations. Previous literature exploring cyberattacks in this field of study has mostly relied on media-derived data and assumed that state actors are necessarily behind these attacks. My dissertation shows that this is not always the case and that especially for DoS attacks it might be more likely that hacking groups or activists launch these attacks during international conflict. Overall, the results of my third study (Chapter 4) question whether governments systematically use DoS attacks at all during international conflict. In this paper, I show that economic sanctions, as one of the likeliest cases where one could expect that the targeted state responds with digital means, appear to be mostly unrelated to an increase in DoS attacks. The results suggest that governments do not launch DoS attacks as a coercive tool to reach concessions. By this, my dissertation empirically supports previous theoretical works on cyber conflict that argue that cyberattacks are an ineffective coercive tool (Rid, 2012; Gartzke, 2013).

Social Movement Literature Finally, the results of my dissertation find only some evidence for the systematic use of DoS attacks as a contention tool. In the first paper (Chapter 2), the main results do not show a systematic increase of DoS attacks on the country during election periods. During such periods, an increase of DoS attacks on the country could have been explained by activists launching DoS attacks on government websites to protest electoral fraud, for example. Although additional models point to a rise in DoS attacks on very authoritarian countries during election periods, it remains unclear how robust these results are. Similarly, the results of the third paper (Chapter 4) point to a contentious use of DoS attacks after sanction impositions only in a few cases. Overall, these results suggest that the use of DoS attacks by activists in autocracies is not as common and that political events rarely trigger, at least, large-scale attacks. This

finding echoes Coleman (2014) who depicts DoS attacks and other hacktivist actions as "weapons of the geek" that is "a modality of politics exercised by a class of privileged and visible actors who often lie at the center of economic life." Translated this means that DoS attacks appear to be no new "weapons of the weak" (Scott, 1985) used by many opposition activists in autocracies, but remains a tool for technologically sophisticated groups.

5.2 Policy Recommendations

Overall, the results of my papers suggest that the censorship use of political DoS attacks is the most pronounced. Although many news and opposition websites already protect themselves from DoS attacks, smaller outlets can often not afford such costly services. Hence, it is advisable to invest in initiatives that distribute this protection also to these outlets. DoS mitigation services such as Google Shield, Deflect, and VirtualRoad are notable initiatives that help vulnerable organizations to protect themselves and that are not driven by economic considerations. Although these and other DoS mitigation services cannot guarantee a 100% protection from DoS attacks, they help in fending off these attacks quickly, making DoS attacks a less harmful weapon against the freedom of information.

More generally, to make it more difficult to conduct DoS attacks, policymakers should invest in efforts to secure Internet devices better. Especially the so-called Internet-of-Things (IoT) is frequently secured badly by inadequate security protocols, and cybercriminals and others can easily compromise these devices, e.g., TVs and security cameras, for malicious purposes. The most famous example of this use is the so-called Mirai botnet. For example, in 2016, perpetrators used this botnet to bring down Dyn, a company that controls much of the Internet's DNS structure. As a consequence, many users in North America and Europe could temporally not access a large share of websites, including Twitter, CNN, and others (Woolf, 2016). Already ongoing initiatives, such as one by CAIDA that makes it harder for perpetrators to spoof their IP address (Lone et al., 2017), are another vital step to make the Internet safer and DoS attacks less effective.

Finally, the results of this dissertation suggest that we should not overemphasize the threat of cyber conflicts. The results of my third paper (Chapter 4) finds that there is no systematic relationship between aggressive foreign policy events, more precisely sanctions, and the development of DoS attacks. More generally, this suggests that DoS and likely other cyberattacks are not as commonly used by governments as many pundits tend to assume. In general, policymakers and think tanks would benefit from discussing cybersecurity issues in a more empirical manner.

5.3 Future Research

While there are several avenues for future research, I believe that the results from my dissertation point to some research paths that would help to falsify or support the dissertation's main findings and advance the study of digital politics.

My dissertation finds the most compelling evidence for the systematic use of DoS attacks as a censoring tool in autocracies. Nevertheless, my studies do not explore the effectiveness and potential consequences of DoS attacks in greater detail. Although additional exploratory models in the second paper (Chapter 3) find only limited evidence for an effect of DoS attacks on changes in reporting made by attacked news websites, these models look on short-term developments only. Future research should more closely investigate the medium and long term impacts of DoS attacks on news and other websites. Besides, different websites and organization types might react differently to DoS attacks. The results of the additional models in the second paper (Chapter 3) suggest that DoS attacks do not pose any threat to protected websites, whereas unprotected websites are more vulnerable. Finally, it may be that obvious and large-scale DoS attacks on websites lead to a backlash effect, increasing interest instead of silencing websites.

In addition to exploring the consequences of attacks, future research should also improve the data collection of DoS attacks, which would enable to more accurately test my theoretical considerations. Regarding the data provided by CAIDA, a logical next step would be to disaggregate DoS attacks from the country-level to exact targets. With this, researchers would get a better understanding of the targets of DoS attacks and could filter out politically relevant attacks already from the raw data. While this is a difficult task for historical analyses, the set-up of a pipeline that does this directly when CAIDA measures attacks would bring research immensely forward. Such an improvement would also allow to more precisely test the proposed theoretical mechanisms. The goal of DoS attacks to censor may be different depending on the website type. For example, the just-in-time censorship mechanism may more likely apply when DoS attacks target live-streams. Besides, researchers could compare media-derived data with DoS attacks on political targets measured by CAIDA, which would allow quantifying media biases. Finally, scientists should use and work with other measurement approaches, e.g., the one proposed in the second paper (Chapter 3) to capture potential DoS attacks actively. Other approaches would be to work together with websites at risk and analyze their log data to infer DoS attacks, collaborate with DoS mitigation services, or ideally, develop ways to monitor DoS attacks by attackers directly allowing to investigate perpetrators as well.

Besides, although the dissertation has focused on the political use of DoS attacks, there are reasons to believe that many of the proposed theoretical considerations also hold for other forms of online censorship, for example, HTTP and Domain Name System filtering, and online contention, e.g., web defacements (Maggi et al., 2018). While recent work

by Roberts (2018) on online censorship in China brought research immensely forward by arguing that censorship works through three different mechanisms, fear, friction, and flooding, empirical studies beyond China are still missing. To advance our understanding of the political drivers and outcomes of Internet censorship, political scientists would greatly benefit from working together with computer scientists on these issues as well (e.g., Weinberg et al., 2017; Pearce et al., 2017; VanderSloot et al., 2018). Furthermore, research on other types of digital information control in autocracies and beyond is still in its infancy. For example, while research has shown that the Russian government uses online bots to manipulate political views (Sanovich, Stukal and Tucker, 2018), the reach and efficiency of such and other tactics remain unknown.

Finally, even though the focus of this dissertation has been on autocracies, the proposed theoretical considerations may travel to democratic countries. For instance, there is evidence that supposedly alt-right activists or sympathizers frequently launched DoS attacks against the website of the social movement "Black Live Matters" in recent years (Ling, 2016). This example shows that activists launch DoS and other cyber actions not only against government websites but highlights that also polarized groups may confront each other in the virtual world. Another aspect, which I did not investigate in my dissertation, is the political use of these attacks against companies and other private organizations to protest against copyright or Internet-related issues.

A

Declaration of Authorship

I hereby declare that I am the sole author of the introduction, the second paper, the third paper, the conclusion, and the accompanying material. The first paper is co-authored with Nils B. Weidmann, Margaret E. Roberts, Mattijs Jonker, Alistair King, and Alberto Dainotti. In the following, I outline the division of labor.

Alistair King, Alberto Dainotti, and Mattijs Jonker prepared the raw data of spoofed DoS attacks for the period of study (2008 – 2016). For a first draft, I post-processed this data (aggregated to a week/country level) and combined it with other political variables of interest. After a first presentation of this project in September 2017, where we initially focused on protest events in autocracies, we moved the focus of the paper to election periods. After this presentation and several discussions with Nils B. Weidmann and Margaret E. Roberts, as well as comments from the IMAPS workshop in 2017, I came up with the idea to additionaly create a variable that measures DoS attacks on newspaper hosting countries. In this task, Mattijs Jonker supported me by determining in which countries news websites are hosted using OpenINTEL.

Afterward, I wrote a second draft with the focus on DoS attacks during election periods, which I presented at three conferences. While I conducted all of the empirical analyses and wrote the largest share of the paper, Nils B. Weidmann and Margaret E. Roberts supported me much in framing and re-writing parts of the paper. This is, in particular, true for the introduction and the conclusion as well as the theoretical section. Furthermore, the three of us worked together on the revisions after the paper was sent to a scientific journal. During this stage, I again conducted all additional analyses, and Mattijs Jonker helped me retrieving additional information regarding hosting pat-

terns of news websites. The version included in this dissertation is the outcome of this cooperation and was published in the *Journal of Conflict Resolution*.

Konstanz, October 2019

Philipp M. Lutscher

B

Supplementary Material For Chapter 1

Political Denial-of-Service Attacks Database (PDOSD)

In this appendix, I briefly describe how I set up the media-based database on politically motivated DoS attacks using newspaper articles retrieved from LexisNexis to hand-code these attacks. While the database records news reports on these attacks, the attacks are aggregated to an event level for Figures 1.1 – 1.4 in the introduction.

Coding Instructions

The coder is provided with a list of newspaper articles that mention Denial-of-Service attacks. These articles are provided in an online repository, in which the coder gradually deletes read articles. The first task is to determine whether the mentioned DoS attack is political. We assume when the target of DoS attacks is either a state actor (e.g., government website), an opposition actor (e.g., opposition blogs, party), or an international political actor (e.g., International Organization, INGO), then the attack is political. Furthermore, incidents where the reason or suspected attacker is political, although the target is private (media organizations or private companies), should be included. Examples for this are attacks on PayPal or on news websites due to political reasons. For this task, a quick skim of the article is sufficient. Overall, we expect that only a small share of the included articles is political. Furthermore, when the articles mention different targets, for example, attacks on opposition websites and government homepages, or targets in different countries, or during distinct periods[1], then the coder should create a new entry for each different attack. Furthermore, when 20 or more articles refer to the same attack, subsequent attacks do not have to be coded more.[2]

When the article is political, the following information must be available. Only then the information will be extracted to a Google form that collects all political relevant news reports about DoS attacks. First, the targeted actor must be filled in, for example, "government". If there is more than one attacked actor, all actors should be filled in and separated by a semicolon. Second, the coder fills in the type of target, which might be (1) a state target (e.g., government), (2) an opposition target (e.g., opposition party, critical newspaper, etc.), (3) an international political target (international NGOs or Organizations), (4) a media target (e.g., news websites, where a critical stance is not clear from the article, or social media providers) and (5) private actors (e.g., PayPal). If they are several actors, the type of the target is the most frequently mentioned actor. For example, when there were DoS attacks against the Tunisian DNS server, central bank, and government websites during the Arab uprising, the type variable would be (1).

[1] When the attacking is reoccurring in the same week, then this can be coded as one attack. If not create two separate entries.

[2] Because the articles are randomly assigned there is no systematic error in deleting these additional articles. Furthermore, it is highly likely that all the sufficient information should be found in up to 20 articles and more articles do not provide any new information.

Lastly, there must be information about the period of the attack. The coder fills in the start and end date of the attack in the following format: DD/MM/YYYY. If the attack only happened on one day, these fields contain the same date. When the date is only vague available, for example, "the DoS attacks started last week", the coder always chooses the first day of the week (Monday) as date. Attacks "over the weekend" start Saturday and end Sunday. When no or only very aggregate information (e.g., last month, year, etc.) about the date is available, or the referred date is in the future, the event report is not to be coded. Furthermore, the coder must copy the name of the newspaper, the publication date, and the unique file code for the articles in separate columns.

Besides this necessary information, additional variables should be coded. If there is no information about these variable, the coder can leave these fields blank. These variables are: First, the attacked country that should be filled in using ISO-3 abbreviations. Second, the targeted service should be filled in. That is either a website (e.g., www.cnn.com), a blog, a chat/email server, social media, a DNS server, or some other server. If there are again multiple targets, separate the services again with semicolons. Third, the attacker actor should be filled in. Please use the extra variable, level of uncertainty, to indicate whether this information is certain (1) or not (0). Fourth, the attacker type should be determined. Attacker types are similar as above (1) state or government-related proxies, e.g., Russian hacker groups, (2) opposition actors, (3) international actors, e.g., *Anonymous* or (4) private actors. Fifth, the suspected reason, and finally, the server location of the target (again with an ISO-3 abbreviation) should be filled in, when this information can be found within the article.

Codebook

- Focus: Political DoS attack
- Unit of Analysis: Political DoS attack event report (by target type)
- Necessary categories:
  - Target actor: Name the attacked actor
  - Target type: Indicate whether the attack was on (1) a state actor, (2) opposition actor, (3) international actor, (4) media actor or (5) private actor
  - Start date: Indicate the start date of the attack
  - End date: Indicate the start date of the attack
- Desired categories (fill in if available):
  - Target country: Name the attacked country
  - Target service: Indicate what was attacked (Blog, chat/email server, social media, DNS server, other kinds of server). Multiple targets separate with ";"
  - Attacker actor: Name the attacking organization/group or country
  - Level of uncertainty (attacker): Please indicate how confident the article is about the attacker (1 = certain, 0 = uncertain)
  - Attacker type: Indicate whether the attack was conducted by (1) a state actor or proxy, (2) opposition actor, (3) international actor or (4) private actor
  - Suspected reason: Indicate the reason for the attack
  - Server Location: Indicate the location of the server
- Automated categories:
  - Newspaper: Copy from article
  - Newspaper date: Copy from article
  - Article ID: Copy from article
- Search Term in LexisNexis: DDoS attack OR DoS attack OR Denial-of-Service attack

Articles to code:	
Year	Number of articles
2008	1114
2009	1769
2010	2543
2011	1529 (6 month) + 1620 (6 month) = 3149
2012	1757 (6 month) + 1470 (6 month) = 3227
2013	2411 (6 month) + 1818 (6 month) = 4229
2014	2134 (6 month) + 2223 (6 month) = 4357
2015	2503 (6 month) + 2382 (6 month) = 4885
2016	2294 (6 month) + 1741 (3 month) + 2508 (1.5 month) + 2290 (1.5 month) = 8833
Total	34106

Coded articles:	
Relevant articles	2602
Number of DoS attacks	681

Table B.1: Temporal development of articles and number of coded DoS attacks.

C

Supplementary Material For Chapter 2

Statistic	N	Mean	St. Dev.	Min	Max
DoS attacks on domestic hosts (ln)	81,840	1.834	2.338	0.000	12.120
DoS attacks on foreign hosts (ln)	28,704	9.526	1.405	0.000	11.993
Autocracy index	73,872	0.432	0.237	0.053	0.926
Election period	84,281	0.049	0.216	0.000	1.000

Table C.1: Summary statistics of main variables

	Model C.2.1 Domestic	Model C.2.2 Domestic	Model C.2.3 Foreign	Model C.2.4 Foreign
Temporal proximity	−0.042	−0.089	0.172***	−0.053
	(0.028)	(0.062)	(0.026)	(0.056)
Temporal proximity × autocracy index		0.158		0.607***
		(0.135)		(0.117)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81840	71280	28704	24960

Table C.2: Relationship between temporal proximity of an election (1 / time to nearest election) dependent on the level of autocracy and DoS attacks (country/week). Note: The election week is set to 1. Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Domestic		Foreign	
	Model C.3.1 Democratic	Model C.3.2 Autocratic	Model C.3.3 Democratic	Model C.3.4 Autocratic
Election period	−0.035	−0.008	−0.048**	0.076***
	(0.019)	(0.023)	(0.017)	(0.020)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	42255	28562	14807	9696

Table C.3: Relationship between election periods and DoS attacks, estimated separately for democratic and autocratic regimes (country/week). Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.4.1 Domestic	Model C.4.2 Domestic	Model C.4.3 Foreign	Model C.4.4 Foreign
Election period	−0.032*	−0.040	−0.020	−0.096***
	(0.014)	(0.030)	(0.012)	(0.026)
Election period × autocracy index		0.037		0.229***
		(0.065)		(0.055)
Conflict events (ln+1)	0.024	0.024	−0.017	−0.016
	(0.013)	(0.013)	(0.010)	(0.010)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81305	70817	28175	24503

Table C.4: Relationship of election period dependent on the level of autocracy with DoS attacks (country/week): Models with conflict variable. Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.5.1 Domestic	Model C.5.2 Domestic	Model C.5.3 Foreign	Model C.5.4 Foreign
Election period	−0.032*	−0.029	−0.020	−0.035*
	(0.014)	(0.020)	(0.012)	(0.018)
Election period × Polity2		−0.009		0.125**
		(0.055)		(0.044)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81305	67528	28175	23382

Table C.5: Relationship of election period dependent on the level of autocracy (Polity2 index) with DoS attacks (country/week). Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.6.1 Domestic	Model C.6.2 Domestic	Model C.6.3 Foreign	Model C.6.4 Foreign
Election period	−0.025	−0.039	−0.009	−0.077**
	(0.015)	(0.030)	(0.012)	(0.025)
Election period × autocracy index		0.035		0.166**
		(0.065)		(0.052)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Country-year time trend	Yes	Yes	Yes	Yes
Num. obs.	70817	70817	24503	24503

Table C.6: Relationship of election period dependent on the level of autocracy with DoS attacks (country/week): Models with time trends. Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.7.1 Domestic	Model C.7.2 Domestic	Model C.7.3 Foreign	Model C.7.4 Foreign
Election period	−0.023	−0.014	−0.020*	−0.078***
	(0.012)	(0.029)	(0.010)	(0.022)
Election period × autocracy index		0.003		0.158***
		(0.057)		(0.046)
Country × year fixed-effects	Yes	Yes	Yes	Yes
Num. obs.	81305	70817	28175	24503

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

Table C.7: Relationship of election periods dependent on the level of autocracy with strong DoS attacks (country/week). Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.8.1 Domestic	Model C.8.2 Domestic	Model C.8.3 Domestic	Model C.8.4 Domestic	Model C.8.5 Foreign	Model C.8.6 Foreign	Model C.8.7 Foreign	Model C.8.8 Foreign
Election period	−0.015	−0.022			−0.003	−0.030		
	(0.014)	(0.031)			(0.009)	(0.018)		
Election period × autocracy index		0.021				0.084*		
		(0.070)				(0.039)		
Election week			0.033	0.003			−0.002	−0.122**
			(0.026)	(0.057)			(0.019)	(0.038)
Election week × autocracy index				0.088				0.314***
				(0.119)				(0.091)
Country × year fixed-effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Num. obs.	80375	70007	80910	70470	27255	23703	28520	24800

Table C.8: Relationship between election periods dependent on the level of autocracy and DoS attacks (country/week): Models with a lagged dependent variables. Note: Lagged dependent variables are not displayed. The number of lags is determined by Durbin-Watson tests. We include as many lags until this test no longer suggests a serious positive AR(1) autocorrelation. For the domestic models, one lag is included, while for the foreign host models, five lags are used for the election period and one for the election week specification. It has to be noted though that tests for higher-order autocorrelation (Breusch-Godfrey tests) still highlight issues with autocorrelation. Inspecting the residuals graphically suggest that these do not seem to follow a systematic trend and highlight that they are relatively small and in the most cases negative (which should lead to *higher* levels of uncertainty for the estimates). Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.9.1 2016 (only)	Model C.9.2 2016 (only)	Model C.9.3 placebo	Model C.9.4 placebo	Model C.9.5 without CDNs	Model C.9.6 without CDNs
Election period	0.006	−0.048	−0.001	0.042	−0.027*	−0.097***
	(0.019)	(0.039)	(0.019)	(0.041)	(0.012)	(0.027)
Election period × autocracy index		0.169*		−0.087		0.215***
		(0.086)		(0.083)		(0.056)
Country × year fixed-effects	Yes	Yes	Yes	Yes	Yes	Yes
Num. obs.	9039.	7863	28175	24503	28175	24503

Table C.9: Relationship between election periods dependent on the level of autocracy and DoS attacks (country/week): Models for attacks on foreign hosts using data from 2016 only, placebo foreign hosts and recalculated index for foreign hosts. Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	Model C.10.1 Domestic	Model C.10.2 Foreign
Election period	0.122*	−0.210***
	(0.050)	(0.048)
Election period × autocracy index	−1.009***	0.915***
	(0.273)	(0.244)
Election period × autocracy index (sq.)	1.197***	−0.755**
	(0.318)	(0.263)
Country × year fixed-effects	Yes	Yes
Num. obs.	70817	24503

Table C.10: Relationship between election periods dependent on the level of autocracy and DoS attacks (country/week): Squared terms interaction models. Note: Robust standard errors clustered at the country-year level in parentheses. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

D

Supplementary Material For Chapter 3

D.1 Summary Statistics and Main Models

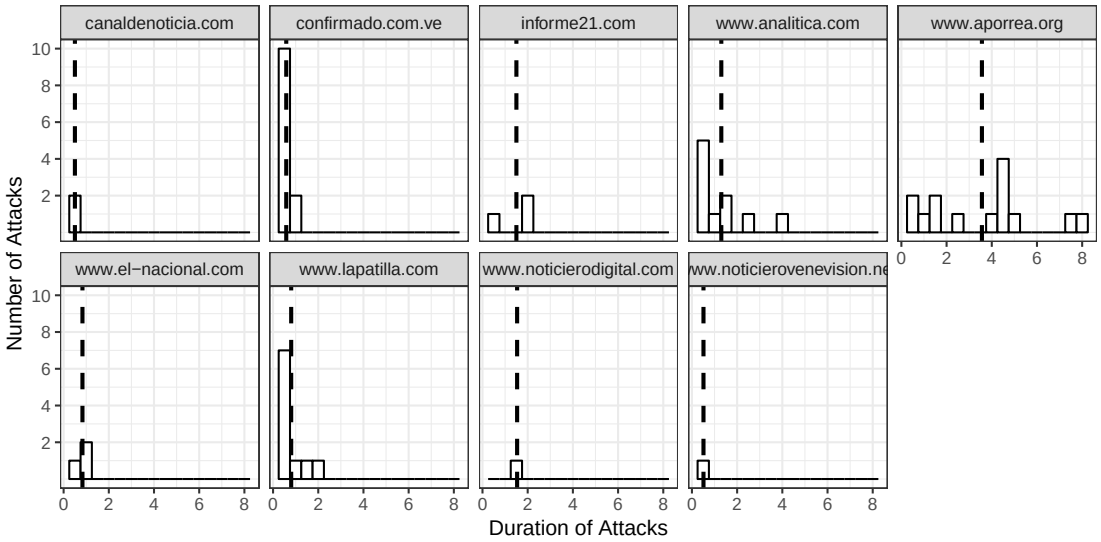

Figure D.1.1: Duration of DoS Attacks on attacked websites per day. Note: The vertical dashed lines show the respective group means. The duration is shown in hours per day. The minimum duration is 30 minutes (one failed measurement), the maximum eight hours (16 failed measurements).

ID	Name	Affiliation	Post-processing worked?	Venezuelan readers?	Comments	Hosted country	Hoster
32	**http://globovision.com/**	private	yes	82.5%		US	CLOUDFLARE
33	https://laradiodelsur.com.ve/	government	n.a.	n.a.		VE	CANTV-NET
34	**http://www.radiofeyalegrianoticias.net/**	private	yes	78%		CA	IWEB
35	http://rnv.gob.ve/	government	n.a.	n.a.		VE	CANTV-NET
36	**http://www.televen.com/**	private	yes	86%	Due to non-structure might include entertaiment/sport news	US	Not known
37	**http://unionradio.net/**	private	yes	68%		US	MICROSOFT
38	**http://www.noticierovenevision.net/**	private	yes	80.4%		US	AMAZON
39	http://vtv.gob.ve/	government	n.a.	n.a.		VE	CANTV-NET
40	http://www.abrebrecha.com/	not known	n.a.	n.a.	Website stopped to work	US	Unified Layer
41	**http://www.analitica.com/**	private	yes	52%		US	CLOUDFLARE
42	**https://www.aporrea.org/**	opposition	yes	87%		US	CLOUDFLARE
43	**https://canaldenoticia.com/**	not known	yes	not known		US	DREAMHOST
44	**http://confirmado.com.ve/**	private	yes	56%		US	GO-DADDY
45	**https://dolartoday.com**	private	yes	37.4%		US	CLOUDFLARE
46	https://elpitazo.com/	private	no	n.a.	Extracting did not work	US	Not known
47	http://www.entornointeligente.com/	private	n.a.	n.a.	News aggregator website	US	CLOUDFLARE
48	**http://elperiodicovenezolano.com/**	not known	yes	73.3%		CA	OVH
49	http://entodonoticias.com/	not known	n.a.	n.a.	Stopped to update content	VE	Patriacell, C.A.
50	**http://informe21.com/**	not known	yes	56%		US	CLOUDFLARE
51	**https://www.lapatilla.com/**	opposition	yes	75%		US	CLOUDFLARE
52	**http://www.notiactual.com**	not known	yes	89%		US	Netrouting AS
53	http://www.noticias.com.ve/	not known	n.a.	n.a.	Stopped to update content	US	MICROSOFT
54	http://www.noticias24.com/	pro-government	n.a.	n.a.	Editors pro-government	US	Rackspace
55	http://www.noticiasdevenezuela.org/	not known	n.a.	n.a.	Website was shut down	US	CLOUDFLARE
56	http://noticiasvenezuela.info/	not known	n.a.	n.a.	Website was shut down	US	11INT
57	**http://www.noticierodigital.com/**	private	yes	83%	Due to non-structure might include entertainment/sport news	US	CLOUDFLARE
58	http://www.notiven.com/	not known	n.a.	n.a.	News aggregator website	US	CLOUDFLARE
59	http://todayvenezuela.com/	not known	n.a.	n.a	English	US	CyrusOne
60	https://venezuelanalysis.com/	private	n.a.	n.a.	English	DE	INTEROUTE
61	**http://www.dinero.com.ve/**	private	yes	67%		VE	Dayco Telecom, C.A.
62	http://enpaiszeta.com/	private	no	n.a.	Extracting did not work	US	GODADDY
63	**http://www.2001.com.ve/**	not known	yes	92%		US	MICROSOFT
64	http://www.elmundo.com.ve/	pro-government	n.a.	n.a.	Merged with http://www.ultimasnoticias.com.ve/ beginning of June	CA	OVH
65	**http://www.el-nacional.com/**	private	yes	78%	Due to non-structure might include entertainment/sport news	US	AMAZON
66	**http://www.eluniversal.com/**	private	yes	80%	Due to non-structure might include entertainment/sport news	CA	OVH
67	http://www.ultimasnoticias.com.ve/	pro-government	n.a.	n.a.		CA	OVH
68	http://www.avn.info.ve/	private	n.a.	n.a.	Scraping did not work	VE	CANTV-NET

Table D.1.1: Assessment of monitored websites. Note: Included website are highlighted in bold. In cases when Content Delivery Networks (CDNs) are used the geo-location refers to the delivery network (Cloudflare, Amazon, Microsoft and Rackspace). The estimates for Venezuelan readers are taken from www.alexa.com.

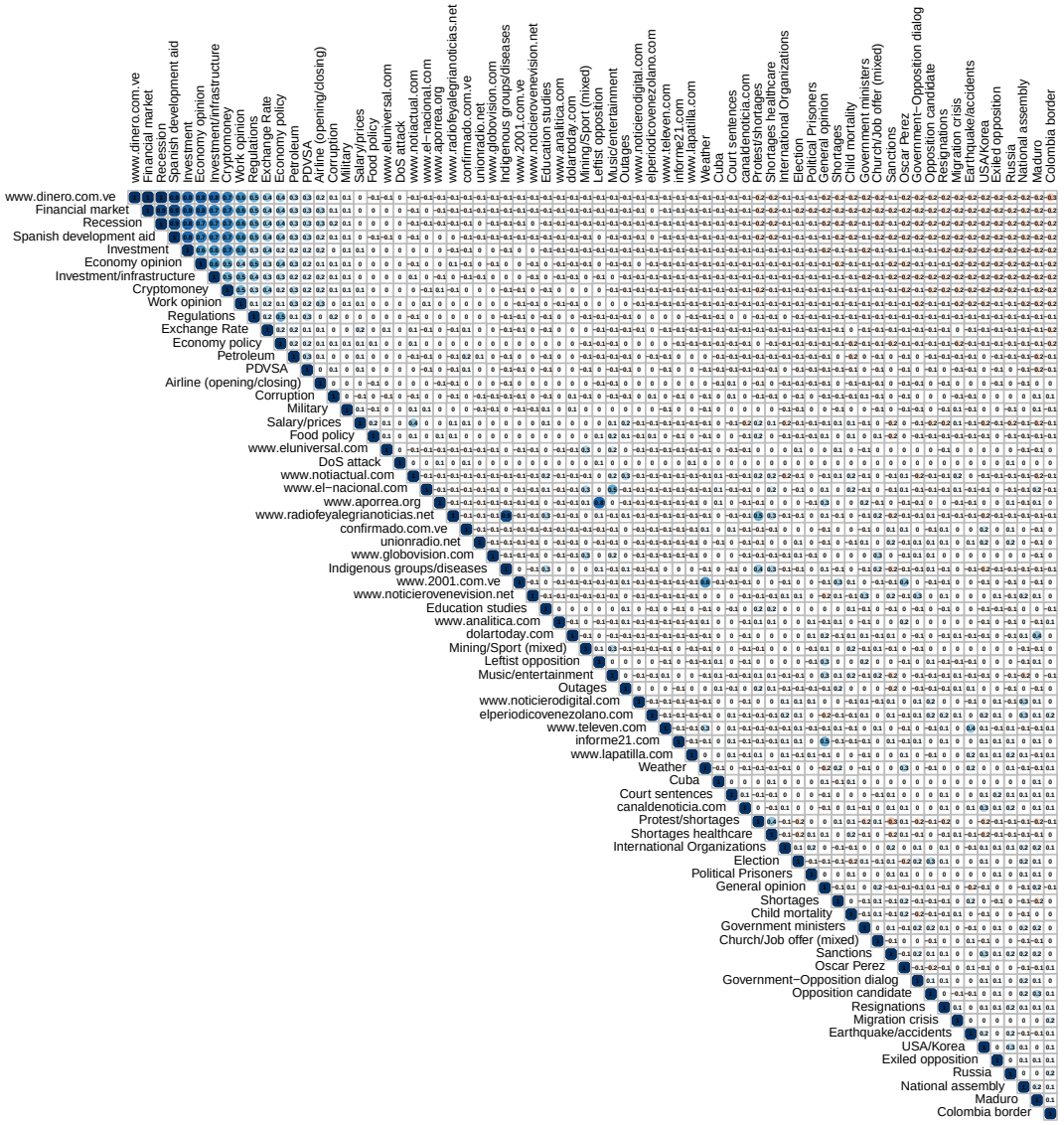

Figure D.1.2: Newspaper/day correlation between topics and websites (in the short-term). Note: The figure is ordered along a principal component analysis, clustering highly collinear topics and websites. Blue dots display a positive correlation, whereas red dots a negative one. Darker shades indicate a stronger correlation.

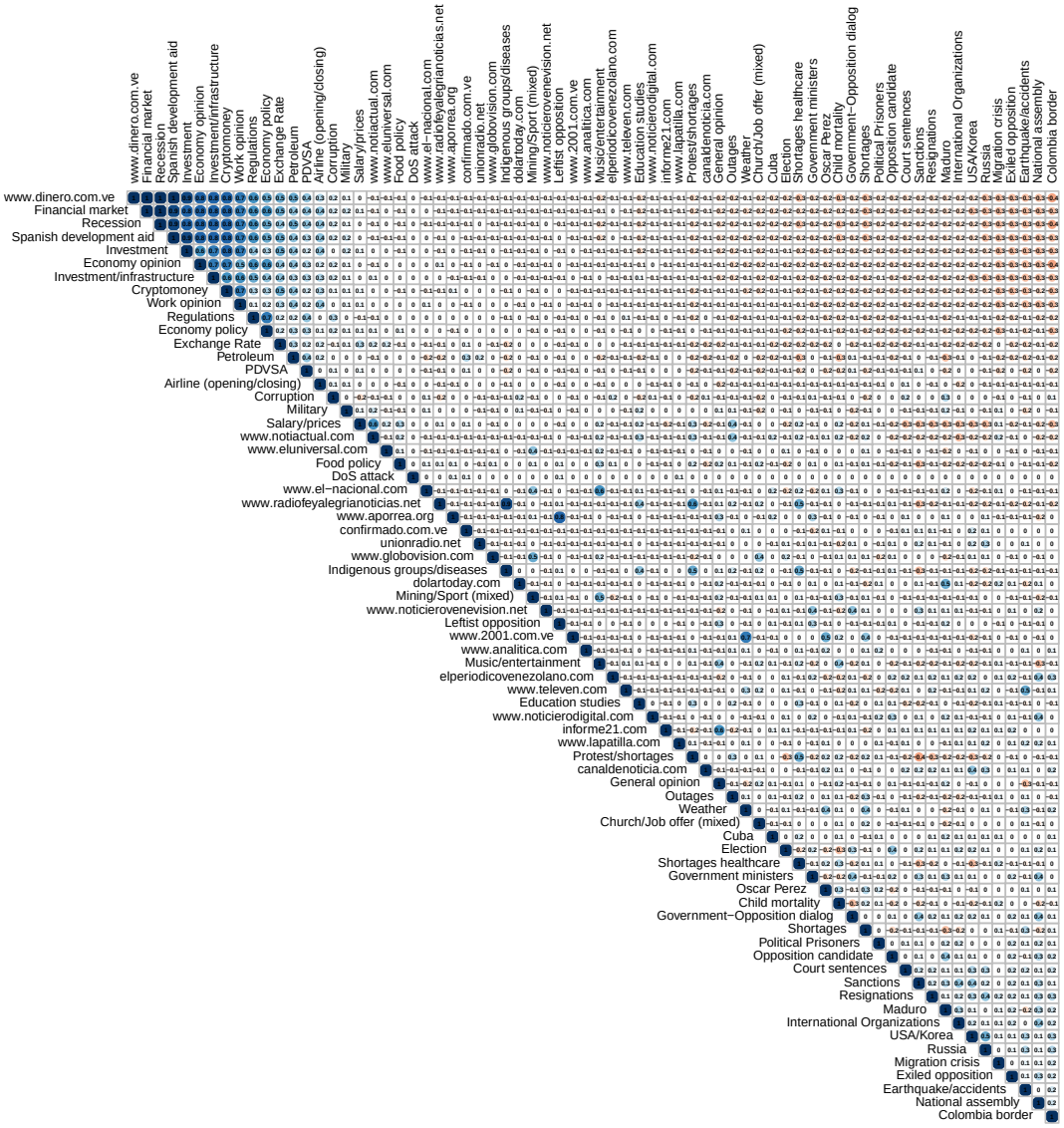

Figure D.1.3: Newspaper/day correlation between topics (in the medium-term) and websites. Note: The figure is ordered along a principal component analysis, clustering highly collinear topics and websites. Blue dots display a positive correlation, whereas red dots a negative one. Darker shades indicate a stronger correlation. The figure shows the same patterns as in Figure D.1.2.

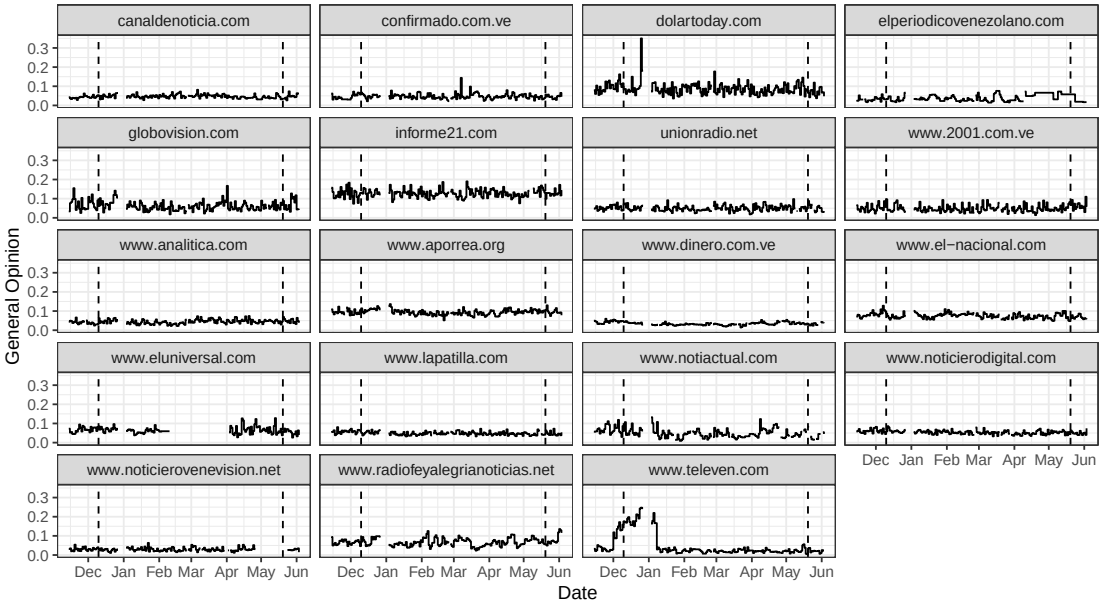

Figure D.1.4: Development of the topic *general opinion* in Venezuela November 2017 - June 2018. Note: The two vertical dashed lines show the municipal election (December 10, 2017) and presidential election (May 20, 2018). Blank periods indicate time periods where the measurement did not work.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.00	0.03	−0.42***	0.29***	0.25***	0.04	−0.42	−0.70*	0.23	0.24	0.03	−0.61***	−0.03	−2.27***	−0.09	0.12	0.11	−0.07	−0.14	−0.83*	0.09	−0.08	0.10
	(0.25)	(0.13)	(0.09)	(0.04)	(0.05)	(0.11)	(0.25)	(0.35)	(0.13)	(0.19)	(0.18)	(0.12)	(0.21)	(0.56)	(0.27)	(0.13)	(0.17)	(0.11)	(0.21)	(0.35)	(0.11)	(0.11)	(0.08)
Number of headlines	0.05**	0.05**	0.05***	0.05**	0.05***	0.05***	0.06***	0.05**	0.05***	0.05**	0.05***	0.07***	0.05**	0.05***	0.05***	0.04**	0.05**	0.05***	0.05**	0.05***	0.05**	0.06**	0.05**
	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.71***	2.71***	2.70***	2.74***	2.67***	2.71***	2.66***	2.63***	2.71***	2.68***	2.71***	2.53***	2.72***	2.60***	2.69***	2.69***	2.71***	2.70***	2.70***	2.66***	2.71***	2.71***	2.72***
	(0.58)	(0.60)	(0.59)	(0.59)	(0.56)	(0.60)	(0.55)	(0.59)	(0.59)	(0.62)	(0.59)	(0.57)	(0.59)	(0.53)	(0.60)	(0.58)	(0.60)	(0.59)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)
AIC	411.27	411.29	407.83	406.48	409.18	411.34	407.56	405.29	410.35	409.40	411.30	401.93	411.20	401.78	410.91	410.38	411.16	410.94	410.48	405.07	411.17	410.93	411.20
BIC	435.96	435.99	432.53	431.17	433.88	436.04	432.25	429.99	435.05	434.09	435.99	426.63	435.90	426.48	435.61	435.08	435.85	435.63	435.17	429.76	435.87	435.63	435.89
Log Likelihood	-201.63	-201.64	-199.92	-199.24	-200.59	-201.67	-199.78	-198.65	-201.17	-200.70	-201.65	-196.97	-201.60	-196.89	-201.46	-201.19	-201.58	-201.47	-201.24	-198.53	-201.59	-201.47	-201.60
Deviance	403.27	403.29	399.83	398.48	401.18	403.34	399.56	397.29	402.35	401.40	403.30	393.93	403.20	393.78	402.91	402.38	403.16	402.94	402.48	397.07	403.17	402.93	403.20
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.34***	0.18	−0.04	0.11	−0.07	−0.14	0.22	0.08	−0.00	0.01	0.06	−0.33*	−0.23	0.43***	0.37***	0.32***	−0.48	0.08	0.21	0.01	−0.14	−0.21	−0.71*
	(0.07)	(0.13)	(0.16)	(0.17)	(0.19)	(0.13)	(0.14)	(0.08)	(0.16)	(0.16)	(0.26)	(0.13)	(0.13)	(0.09)	(0.10)	(0.07)	(0.39)	(0.19)	(0.14)	(0.19)	(0.13)	(0.21)	(0.34)
Number of headlines	0.05***	0.05***	0.05***	0.05***	0.05***	0.05**	0.05***	0.05***	0.05**	0.05***	0.05**	0.05***	0.05***	0.06***	0.05***	0.05***	0.06***	0.05**	0.05***	0.05**	0.05**	0.05***	0.06***
	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)
DoS attack (t-1)	2.58***	2.67***	2.70***	2.69***	2.69***	2.73***	2.60***	2.79***	2.71***	2.71***	2.72***	2.67***	2.72***	2.61***	2.66***	2.67***	2.60***	2.71***	2.71***	2.71***	2.70***	2.72***	2.59***
	(0.56)	(0.58)	(0.59)	(0.58)	(0.59)	(0.58)	(0.57)	(0.61)	(0.60)	(0.60)	(0.60)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)	(0.53)	(0.60)	(0.60)	(0.60)	(0.60)	(0.60)	(0.55)
AIC	403.87	410.26	411.06	411.15	410.98	410.52	409.80	411.46	411.26	411.28	411.23	409.20	409.80	403.93	407.58	406.02	406.74	411.14	410.37	411.28	410.42	409.96	405.12
BIC	428.57	435.07	435.76	435.85	435.67	435.21	434.58	436.16	435.95	435.97	435.93	433.90	434.50	428.62	432.27	430.71	431.44	435.84	435.07	435.98	435.12	434.66	429.82
Log Likelihood	-197.94	-201.19	-201.53	-201.58	-201.49	-201.26	-200.94	-201.73	-201.63	-201.64	-201.62	-200.60	-200.90	-197.96	-199.79	-199.01	-199.37	-201.57	-201.19	-201.64	-201.21	-200.98	-198.56
Deviance	395.87	402.38	403.06	403.15	402.98	402.52	401.89	403.46	403.26	403.28	403.23	401.20	401.80	395.93	399.58	398.02	398.74	403.14	402.37	403.28	402.42	401.96	397.12
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.1.2: Penalized logistic regression results - short-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.17	0.22	−0.37***	0.28***	−0.01	0.24***	−0.45*	−0.90**	0.11	0.38**	0.05	−0.45*	0.21*	0.02	−0.21	−0.36*	−1.08***	0.01	−0.09	0.03	0.19**
	(0.24)	(0.10)	(0.06)	(0.04)	(0.08)	(0.04)	(0.18)	(0.27)	(0.25)	(0.14)	(0.19)	(0.20)	(0.10)	(0.21)	(0.18)	(0.15)	(0.29)	(0.12)	(0.14)	(0.08)	(0.07)
DoS attack (t-1)	1.89***	1.88***	1.92***	1.92***	1.89***	1.88***	1.84***	1.78***	1.90***	1.89***	1.88***	1.90***	1.85***	1.89***	1.88***	1.90***	1.82***	1.89***	1.88***	1.89***	1.85***
	(0.40)	(0.40)	(0.39)	(0.40)	(0.40)	(0.40)	(0.38)	(0.41)	(0.41)	(0.40)	(0.40)	(0.40)	(0.39)	(0.41)	(0.41)	(0.39)	(0.41)	(0.40)	(0.41)	(0.40)	(0.41)
AIC	398.89	398.70	397.14	396.05	399.09	399.21	396.44	392.52	399.54	395.32	399.28	397.72	398.68	399.31	398.34	397.13	391.56	399.20	399.01	399.18	397.71
BIC	528.54	528.35	526.79	525.70	528.74	528.86	526.09	522.17	529.20	524.97	528.93	527.37	528.33	528.96	527.99	526.79	521.21	528.85	528.66	528.83	527.36
Log Likelihood	-178.44	-178.35	-177.57	-177.02	-178.55	-178.60	-177.22	-175.26	-178.77	-176.66	-178.64	-177.86	-178.34	-178.65	-178.17	-177.57	-174.78	-178.60	-178.50	-178.59	-177.85
Deviance	356.89	356.70	355.14	354.05	357.09	357.21	354.44	350.52	357.54	353.32	357.28	355.72	356.68	357.31	356.34	355.13	349.56	357.20	357.01	357.18	355.71
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.00	0.00	0.47**	0.30**	−0.16	−0.25	0.08	−0.13	−0.09	0.32	−0.06	−0.31**	0.30	0.27***	0.32**	0.08	0.29**	0.04	0.16	−0.17	−0.54**
	(0.13)	(0.12)	(0.16)	(0.10)	(0.14)	(0.25)	(0.06)	(0.21)	(0.14)	(0.28)	(0.14)	(0.10)	(0.18)	(0.03)	(0.11)	(0.19)	(0.08)	(0.15)	(0.17)	(0.21)	(0.21)
DoS attack (t-1)	1.89***	1.89***	1.83***	1.91***	1.92***	1.85***	1.88***	1.87***	1.88***	1.92***	1.89***	1.93***	1.88***	1.89***	1.87***	1.89***	1.88***	1.89***	1.88***	1.89***	1.87***
	(0.40)	(0.40)	(0.36)	(0.41)	(0.38)	(0.42)	(0.41)	(0.39)	(0.40)	(0.40)	(0.40)	(0.41)	(0.41)	(0.40)	(0.43)	(0.40)	(0.40)	(0.40)	(0.40)	(0.41)	(0.38)
AIC	399.17	399.23	396.58	398.46	398.92	397.57	399.45	398.64	398.98	397.70	399.30	397.63	397.53	398.11	396.70	399.35	397.91	399.25	399.28	398.51	396.73
BIC	528.82	528.88	526.23	528.11	528.57	527.22	529.10	528.30	528.63	527.35	528.95	527.29	527.18	527.76	526.35	529.00	527.56	528.90	528.93	528.16	526.38
Log Likelihood	-178.59	-178.61	-177.29	-178.23	-178.46	-177.79	-178.73	-178.32	-178.49	-177.85	-178.65	-177.82	-177.77	-178.06	-177.35	-178.68	-177.95	-178.63	-178.64	-178.25	-177.37
Deviance	357.17	357.23	354.58	356.46	356.92	355.57	357.45	356.64	356.98	355.70	357.30	355.63	355.53	356.11	354.70	357.35	355.91	357.25	357.28	356.51	354.73
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.1.3: Penalized logistic regression results - short-term models (newspaper fixed effects). Note: Newspaper fixed are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.18	0.10	−0.65***	0.25***	−0.11	0.14	−0.27*	−0.74***	0.27	0.39**	−0.18	−0.44**	0.09	0.35***	−0.26	−0.13	−0.93***	0.08	−0.18	0.05	0.20
	(0.17)	(0.11)	(0.09)	(0.04)	(0.12)	(0.08)	(0.12)	(0.21)	(0.22)	(0.13)	(0.19)	(0.15)	(0.09)	(0.10)	(0.13)	(0.19)	(0.19)	(0.07)	(0.12)	(0.10)	(0.12)
DoS attack (t-1)	1.40***	1.39***	1.42***	1.44***	1.39***	1.38***	1.37***	1.32***	1.41***	1.43***	1.39***	1.40***	1.38***	1.41***	1.35***	1.40***	1.37***	1.38***	1.39***	1.39***	1.35***
	(0.36)	(0.37)	(0.34)	(0.34)	(0.37)	(0.36)	(0.35)	(0.36)	(0.37)	(0.36)	(0.37)	(0.36)	(0.36)	(0.38)	(0.38)	(0.35)	(0.37)	(0.36)	(0.37)	(0.36)	(0.38)
AIC	424.39	424.67	420.25	422.60	424.21	424.86	423.78	420.73	424.97	421.58	424.10	423.22	424.70	424.54	423.50	424.52	419.72	424.69	424.10	424.68	423.19
BIC	696.04	696.32	691.90	694.25	695.86	696.51	695.43	692.38	696.62	693.23	695.75	694.87	696.35	696.19	695.15	696.17	691.37	696.34	695.75	696.33	694.84
Log Likelihood	-168.19	-168.34	-166.12	-167.30	-168.11	-168.43	-167.89	-166.36	-168.49	-166.79	-168.05	-167.61	-168.35	-168.27	-167.75	-168.26	-165.86	-168.34	-168.05	-168.34	-167.59
Deviance	336.39	336.67	332.25	334.60	336.21	336.86	335.78	332.73	336.97	333.58	336.10	335.22	336.70	336.54	335.50	336.52	331.72	336.69	336.10	336.68	335.19
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.09	−0.02	0.53***	0.27***	−0.33*	−0.25	0.09*	−0.05	−0.04	0.34	−0.00	−0.40***	0.32	0.16**	0.35***	0.11	0.26**	0.11	0.19	−0.41**	−0.35*
	(0.06)	(0.13)	(0.09)	(0.08)	(0.15)	(0.19)	(0.04)	(0.20)	(0.09)	(0.25)	(0.10)	(0.10)	(0.18)	(0.05)	(0.10)	(0.14)	(0.09)	(0.11)	(0.17)	(0.14)	(0.15)
DoS attack (t-1)	1.37***	1.39***	1.31***	1.42***	1.43***	1.39***	1.38***	1.38***	1.39***	1.42***	1.39***	1.45***	1.40***	1.40***	1.38***	1.39***	1.40***	1.39***	1.38***	1.37***	1.39***
	(0.37)	(0.36)	(0.33)	(0.37)	(0.35)	(0.35)	(0.37)	(0.36)	(0.36)	(0.34)	(0.36)	(0.37)	(0.37)	(0.36)	(0.37)	(0.37)	(0.36)	(0.36)	(0.36)	(0.38)	(0.35)
AIC	424.68	424.64	421.92	424.07	423.64	423.36	424.07	424.58	424.73	423.29	424.00	422.56	422.64	424.49	421.52	424.96	424.04	424.65	424.79	422.26	423.71
BIC	696.33	696.29	693.57	695.72	695.29	695.01	696.02	696.23	696.38	694.94	696.55	694.21	694.29	696.14	693.17	696.61	695.69	696.30	696.44	693.91	695.36
Log Likelihood	-168.34	-168.32	-166.96	-168.03	-167.82	-167.68	-168.48	-168.29	-168.36	-167.64	-168.45	-167.28	-167.32	-168.25	-166.76	-168.48	-168.02	-168.33	-168.40	-167.13	-167.86
Deviance	336.68	336.64	333.92	336.07	335.64	335.36	336.97	336.58	336.73	335.29	336.90	334.56	334.64	336.49	333.52	336.96	336.04	336.65	336.79	334.26	335.71
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.1.4: Penalized logistic regression results - short-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.54	−0.08	−0.90***	0.52***	0.03	0.05	−0.14*	−0.67***	0.12	0.23*	−0.29**	−0.42***	0.04	0.28	−0.41***	0.04	−0.49***	−0.09	−0.63***	0.25*	0.08
	(0.29)	(0.09)	(0.11)	(0.05)	(0.14)	(0.07)	(0.07)	(0.14)	(0.15)	(0.10)	(0.07)	(0.11)	(0.12)	(0.17)	(0.09)	(0.19)	(0.11)	(0.17)	(0.08)	(0.13)	(0.06)
DoS attack (t-1)	2.88***	2.84***	2.84***	2.96***	2.84***	2.83***	2.82***	2.75***	2.83***	2.84***	2.84***	2.86***	2.82***	2.85***	2.82***	2.82***	2.84***	2.85***	2.86***	2.90***	2.82***
	(0.45)	(0.42)	(0.38)	(0.39)	(0.41)	(0.42)	(0.41)	(0.40)	(0.42)	(0.42)	(0.41)	(0.43)	(0.44)	(0.44)	(0.46)	(0.41)	(0.43)	(0.44)	(0.43)	(0.40)	(0.41)
AIC	347.42	349.43	342.13	344.91	349.38	349.80	349.17	346.88	349.88	348.92	348.59	347.19	349.49	349.21	346.82	349.51	347.79	349.23	346.08	348.75	349.04
BIC	742.54	744.56	737.26	740.04	744.50	744.93	744.29	742.01	745.00	744.05	743.71	742.32	744.62	744.34	741.95	744.64	742.92	744.35	741.21	743.87	744.16
Log Likelihood	-109.71	-110.72	-107.07	-108.46	-110.69	-110.90	-110.58	-109.44	-110.94	-110.46	-110.29	-109.60	-110.75	-110.61	-109.41	-110.76	-109.89	-110.61	-109.04	-110.37	-110.52
Deviance	219.42	221.43	214.13	216.91	221.38	221.80	221.17	218.88	221.88	220.92	220.59	219.19	221.49	221.21	218.82	221.51	219.79	221.23	218.08	220.75	221.04
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.19*	0.31*	0.49***	0.22**	−0.78***	0.21	0.48***	0.03	0.04	0.29	0.01	−0.53***	0.52***	0.28***	0.24**	0.24*	−0.19*	0.24*	0.30**	−0.41**	−0.41**
	(0.09)	(0.14)	(0.13)	(0.08)	(0.14)	(0.13)	(0.07)	(0.13)	(0.07)	(0.15)	(0.06)	(0.11)	(0.13)	(0.08)	(0.08)	(0.12)	(0.09)	(0.12)	(0.10)	(0.13)	(0.15)
DoS attack (t-1)	2.90***	2.88***	2.67***	2.80***	2.94***	2.82***	2.92***	2.83***	2.83***	2.78***	2.83***	2.93***	2.89***	2.86***	2.79***	2.83***	2.85***	2.86***	2.84***	2.77***	2.78***
	(0.42)	(0.44)	(0.40)	(0.42)	(0.42)	(0.43)	(0.42)	(0.42)	(0.42)	(0.40)	(0.42)	(0.40)	(0.43)	(0.41)	(0.44)	(0.43)	(0.41)	(0.42)	(0.41)	(0.44)	(0.40)
AIC	348.96	348.91	347.52	348.67	345.51	348.90	346.65	349.25	349.65	348.51	349.72	346.59	342.70	347.95	348.44	349.45	348.92	348.69	348.30	347.51	348.35
BIC	744.09	744.03	742.65	743.80	740.63	744.03	741.77	744.37	744.77	743.64	744.85	741.72	737.83	743.08	743.57	744.57	744.04	743.82	743.43	742.63	743.48
Log Likelihood	-110.48	-110.45	-109.76	-110.33	-108.75	-110.45	-109.32	-110.62	-110.82	-110.25	-110.86	-109.30	-107.35	-109.98	-110.22	-110.72	-110.46	-110.35	-110.15	-109.75	-110.18
Deviance	220.96	220.91	219.52	220.67	217.51	220.90	218.65	221.25	221.65	220.51	221.72	218.59	214.70	219.95	220.44	221.45	220.92	220.69	220.30	219.51	220.35
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.1.5: Penalized logistic regression results - short-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.05	−0.07	−0.45*	0.27**	0.36***	−0.11	−0.17	−0.15	0.22	0.07	0.08	−0.63***	−0.02	−2.87***	−0.35	0.06	0.39***	−0.01	−0.18	0.02	0.22	−0.23	0.21
	(0.25)	(0.27)	(0.21)	(0.08)	(0.08)	(0.21)	(0.20)	(0.22)	(0.17)	(0.14)	(0.20)	(0.12)	(0.23)	(0.74)	(0.34)	(0.12)	(0.11)	(0.14)	(0.16)	(0.24)	(0.12)	(0.23)	(0.17)
Number of headlines	0.05**	0.05**	0.06***	0.05**	0.06***	0.05**	0.05***	0.05**	0.05***	0.05**	0.05**	0.07***	0.05**	0.06***	0.05***	0.05**	0.05***	0.05***	0.05**	0.05**	0.06**	0.05**	0.05**
	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)
DoS attack (t-1)	2.71***	2.71***	2.66***	2.65***	2.64***	2.71***	2.67***	2.71***	2.69***	2.70***	2.70***	2.45***	2.71***	2.54***	2.65***	2.69***	2.64***	2.70***	2.70***	2.72**	2.70**	2.68***	2.70***
	(0.60)	(0.59)	(0.58)	(0.62)	(0.55)	(0.59)	(0.58)	(0.60)	(0.59)	(0.60)	(0.59)	(0.50)	(0.60)	(0.56)	(0.60)	(0.58)	(0.59)	(0.59)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)
AIC	411.26	411.01	407.84	408.19	405.02	410.68	410.28	410.67	410.47	411.14	411.20	401.06	411.21	401.90	408.86	410.97	406.55	411.22	410.13	411.28	410.02	410.05	409.59
BIC	435.95	435.70	432.54	432.88	429.72	435.37	434.98	435.36	435.16	435.83	435.89	425.75	435.91	426.59	433.56	435.67	431.24	435.91	434.82	435.97	434.72	434.74	434.69
Log Likelihood	-201.63	-201.50	-199.92	-200.09	-198.51	-201.34	-201.14	-201.34	-201.24	-201.57	-201.60	-196.53	-201.61	-196.95	-200.43	-201.49	-199.27	-201.61	-201.06	-201.64	-201.01	-201.02	-201.00
Deviance	403.28	403.01	399.84	400.19	397.02	402.68	402.28	402.67	402.47	403.14	403.20	393.06	403.21	393.90	400.86	402.97	398.55	403.22	402.13	403.28	402.03	402.05	401.99
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.31*	0.33*	−0.19	−0.15	−0.13	−0.01	0.50***	0.08	0.23*	0.02	0.11	−1.00*	−0.20	0.37*	0.24*	0.28***	−0.84*	−0.12	0.19	−0.33	−0.14	0.11	−1.02***
	(0.13)	(0.14)	(0.14)	(0.14)	(0.17)	(0.15)	(0.12)	(0.15)	(0.10)	(0.24)	(0.16)	(0.44)	(0.19)	(0.16)	(0.10)	(0.08)	(0.36)	(0.20)	(0.17)	(0.19)	(0.09)	(0.16)	(0.26)
Number of headlines	0.05***	0.06***	0.05***	0.05**	0.05***	0.05**	0.06***	0.05***	0.05***	0.05***	0.05**	0.06***	0.05***	0.06***	0.05***	0.05***	0.08***	0.05**	0.05**	0.05**	0.05**	0.05**	0.06***
	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)
DoS attack (t-1)	2.60***	2.69***	2.67***	2.72***	2.71***	2.71***	2.58***	2.70***	2.68***	2.71***	2.70***	2.60***	2.68***	2.61***	2.64***	2.64***	2.56***	2.72***	2.69***	2.70**	2.70**	2.68***	2.51***
	(0.54)	(0.58)	(0.56)	(0.60)	(0.61)	(0.60)	(0.52)	(0.61)	(0.59)	(0.60)	(0.60)	(0.59)	(0.60)	(0.58)	(0.60)	(0.60)	(0.48)	(0.59)	(0.59)	(0.60)	(0.60)	(0.57)	(0.55)
AIC	407.26	407.76	409.91	410.52	410.54	411.18	401.73	411.26	409.73	411.27	411.01	405.55	410.20	406.46	409.05	409.14	400.21	410.72	410.54	409.13	410.41	411.01	401.96
BIC	431.96	432.45	434.60	435.21	435.23	435.88	426.42	435.95	434.43	435.97	435.70	430.24	434.89	431.16	433.74	433.84	424.90	435.41	435.23	433.82	435.10	435.70	426.65
Log Likelihood	-199.63	-199.88	-200.95	-201.26	-201.27	-201.59	-196.86	-201.63	-200.87	-201.64	-201.50	-198.77	-201.10	-199.23	-200.52	-200.57	-196.10	-201.36	-201.27	-200.56	-201.20	-201.50	-196.98
Deviance	399.26	399.76	401.91	402.52	402.54	403.18	393.73	403.26	401.73	403.27	403.01	397.55	402.20	398.46	401.05	401.14	392.21	402.72	402.54	401.13	402.41	403.01	393.96
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.1.6: Penalized logistic regression results - medium-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.09	0.17	−0.16	0.16	0.05	−0.01	−0.05	0.01	−0.83***	0.20	0.22	−0.77	0.35**	−0.54	0.38**	−0.26**	0.04	0.16	−0.33	0.08	−0.02
	(0.31)	(0.15)	(0.16)	(0.09)	(0.14)	(0.13)	(0.14)	(0.26)	(0.24)	(0.11)	(0.19)	(0.41)	(0.08)	(0.36)	(0.12)	(0.10)	(0.20)	(0.20)	(0.19)	(0.15)	(0.12)
DoS attack (t-1)	2.06***	2.06***	2.05***	2.02***	2.06***	2.06***	2.06***	2.06***	2.03***	2.05***	2.05***	2.03***	2.05***	2.00***	2.06***	2.03**	2.07***	2.05***	2.02***	2.06***	2.06***
	(0.37)	(0.36)	(0.36)	(0.40)	(0.36)	(0.36)	(0.36)	(0.39)	(0.36)	(0.36)	(0.35)	(0.32)	(0.36)	(0.38)	(0.35)	(0.35)	(0.36)	(0.38)	(0.36)	(0.37)	(0.36)
AIC	412.64	412.47	412.24	411.91	412.55	412.77	412.56	412.74	411.75	412.05	412.18	410.52	411.11	410.63	411.15	411.21	412.78	412.37	411.10	412.53	412.41
BIC	542.93	542.75	542.53	542.19	542.83	543.06	542.85	543.03	542.03	542.34	542.47	540.80	541.39	540.91	541.43	541.50	543.07	542.66	541.39	542.82	542.70
Log Likelihood	-185.32	-185.23	-185.12	-184.95	-185.27	-185.39	-185.28	-185.37	-184.87	-185.03	-185.09	-184.26	-184.55	-184.31	-184.57	-184.61	-185.39	-185.19	-184.55	-185.27	-185.21
Deviance	370.64	370.47	370.24	369.91	370.55	370.77	370.56	370.74	369.75	370.05	370.18	368.52	369.11	368.63	369.15	369.21	370.78	370.37	369.10	370.53	370.41
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.20	−0.33	−0.25*	0.75***	0.34	0.17	0.10	0.10	−0.19	0.58***	−0.29	−0.20	−0.01	0.14**	−0.03	0.00	−0.05	−0.27*	−0.37	0.43*	−0.55
	(0.21)	(0.21)	(0.10)	(0.20)	(0.19)	(0.28)	(0.13)	(0.14)	(0.16)	(0.11)	(0.17)	(0.16)	(0.08)	(0.05)	(0.13)	(0.19)	(0.16)	(0.13)	(0.24)	(0.19)	(0.36)
DoS attack (t-1)	2.06***	2.05***	2.05***	1.97***	2.07***	2.08***	2.05***	2.05***	2.05***	2.00***	2.04***	2.05***	2.06***	2.04***	2.07***	2.06***	2.06***	2.06***	2.03***	2.00***	2.03***
	(0.37)	(0.34)	(0.37)	(0.26)	(0.36)	(0.36)	(0.36)	(0.38)	(0.36)	(0.35)	(0.35)	(0.37)	(0.36)	(0.38)	(0.36)	(0.37)	(0.36)	(0.36)	(0.40)	(0.26)	(0.33)
AIC	412.27	410.78	412.25	406.33	412.86	412.20	412.63	412.32	412.00	408.88	412.15	412.17	412.52	412.33	412.52	412.59	412.53	411.99	411.39	408.69	410.89
BIC	542.55	541.07	542.54	536.62	543.15	542.48	542.91	542.60	542.29	539.17	542.44	542.35	542.81	542.62	542.81	542.88	542.82	542.27	541.68	538.98	541.18
Log Likelihood	-185.13	-184.39	-185.12	-182.17	-185.43	-185.10	-185.31	-185.16	-185.00	-183.44	-185.07	-185.03	-185.26	-185.17	-185.26	-185.30	-185.27	-184.99	-184.70	-183.35	-184.45
Deviance	370.27	368.78	370.25	364.33	370.86	370.20	370.63	370.32	370.00	366.88	370.15	370.07	370.52	370.33	370.52	370.59	370.53	369.99	369.39	366.69	368.89
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.1.7: Penalized logistic regression results - medium-term models (newspaper fixed effects). Note: Newspaper effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.01	0.25*	−0.52	−0.24*	0.03	0.09	0.38***	0.53***	−0.52*	−0.04	−0.58***	−6.76*	0.18	0.23	0.63***	0.28**	0.51***	0.35*	−0.33	−0.03	−0.13
	(0.21)	(0.11)	(0.29)	(0.10)	(0.16)	(0.09)	(0.08)	(0.11)	(0.21)	(0.21)	(0.17)	(0.31)	(0.15)	(0.17)	(0.12)	(0.09)	(0.07)	(0.14)	(0.20)	(0.10)	(0.14)
DoS attack (t-1)	1.54***	1.53***	1.49***	1.56***	1.54***	1.53***	1.52***	1.55***	1.53***	1.54***	1.49***	1.50***	1.55**	1.54***	1.55***	1.54***	1.52***	1.52***	1.51***	1.54***	1.54***
	(0.32)	(0.33)	(0.33)	(0.32)	(0.33)	(0.33)	(0.33)	(0.32)	(0.32)	(0.32)	(0.34)	(0.27)	(0.32)	(0.32)	(0.31)	(0.33)	(0.34)	(0.33)	(0.31)	(0.32)	(0.32)
AIC	437.91	437.34	436.05	436.62	437.65	437.94	436.76	436.47	437.43	437.75	435.56	435.71	437.49	437.97	434.45	437.67	436.62	436.86	436.87	437.61	437.31
BIC	710.89	710.32	709.03	709.60	710.63	710.93	709.74	709.45	710.41	710.73	708.54	708.69	710.47	710.95	707.43	710.65	709.60	709.84	709.85	710.59	710.30
Log Likelihood	-174.95	-174.67	-174.02	-174.31	-174.82	-174.97	-174.38	-174.23	-174.71	-174.88	-173.78	-173.85	-174.74	-174.99	-173.22	-174.83	-174.31	-174.43	-174.44	-174.80	-174.66
Deviance	349.91	349.34	348.05	348.62	349.65	349.94	348.76	348.47	349.43	349.75	347.56	347.71	349.49	349.97	346.45	349.67	348.62	348.86	348.87	349.61	349.31
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.39***	0.07	−0.42***	0.85***	−0.09	0.69***	0.13	0.11	0.00	0.92***	−0.38*	0.11	−0.21**	−0.18*	−0.07	0.17	−0.54***	−0.26	−0.46*	0.44***	0.12
	(0.08)	(0.24)	(0.12)	(0.20)	(0.27)	(0.10)	(0.11)	(0.10)	(0.11)	(0.24)	(0.18)	(0.20)	(0.07)	(0.08)	(0.20)	(0.20)	(0.14)	(0.19)	(0.19)	(0.11)	(0.11)
DoS attack (t-1)	1.53***	1.54***	1.51***	1.45***	1.53***	1.51***	1.53***	1.52***	1.54***	1.45***	1.51***	1.54***	1.52***	1.54***	1.54***	1.53***	1.54***	1.54***	1.53***	1.53***	1.54***
	(0.32)	(0.33)	(0.34)	(0.24)	(0.34)	(0.29)	(0.33)	(0.33)	(0.32)	(0.30)	(0.32)	(0.32)	(0.33)	(0.32)	(0.31)	(0.33)	(0.31)	(0.32)	(0.33)	(0.28)	(0.33)
AIC	436.62	437.84	436.77	430.98	437.90	433.03	437.52	437.36	437.78	432.05	437.02	437.94	436.94	437.13	437.50	437.77	435.80	437.21	436.32	436.37	438.28
BIC	709.60	710.82	709.76	703.97	710.88	706.01	710.50	710.34	710.76	705.03	710.00	710.92	709.92	710.11	710.48	710.75	708.78	710.19	709.31	709.35	711.26
Log Likelihood	-174.31	-174.92	-174.39	-171.49	-174.95	-172.51	-174.76	-174.68	-174.89	-172.02	-174.51	-174.97	-174.47	-174.57	-174.75	-174.88	-173.90	-174.60	-174.16	-174.19	-175.14
Deviance	348.62	349.84	348.77	342.98	349.90	345.03	349.52	349.36	349.78	344.05	349.02	349.94	348.94	349.13	349.50	349.77	347.80	349.21	348.32	348.37	350.28
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.1.8: Penalized logistic regression results - medium-term models (newspaper and week fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.10	0.18	−0.79**	−0.15	0.24	0.14	0.35***	0.46***	−0.06	0.04	−0.37***	−0.40*	0.13	0.01	0.45***	0.03	0.33***	0.40*	0.04	0.01	−0.21
	(0.24)	(0.13)	(0.26)	(0.09)	(0.13)	(0.10)	(0.10)	(0.10)	(0.11)	(0.17)	(0.08)	(0.16)	(0.11)	(0.19)	(0.08)	(0.09)	(0.05)	(0.17)	(0.10)	(0.06)	(0.14)
DoS attack (t-1)	2.94***	2.96***	2.92***	2.92***	2.98***	2.96***	2.89***	2.90***	2.94***	2.94***	2.90***	2.88***	2.92**	2.94***	2.95***	2.93**	2.92***	2.89***	2.95***	2.94***	2.94***
	(0.38)	(0.39)	(0.38)	(0.38)	(0.41)	(0.38)	(0.41)	(0.37)	(0.39)	(0.38)	(0.39)	(0.35)	(0.40)	(0.39)	(0.38)	(0.38)	(0.40)	(0.42)	(0.39)	(0.39)	(0.39)
AIC	353.76	353.62	350.56	353.43	353.33	353.96	352.71	352.29	354.13	353.99	352.97	352.85	353.68	353.91	351.66	353.72	353.32	352.56	354.01	353.85	352.97
BIC	750.82	750.69	747.62	750.49	750.39	751.02	749.77	749.35	751.20	751.05	750.03	749.91	750.74	750.97	748.73	750.78	750.39	749.63	751.07	750.91	750.04
Log Likelihood	-112.88	-112.81	-111.28	-112.71	-112.66	-112.98	-112.35	-112.14	-113.07	-112.99	-112.48	-112.42	-112.84	-112.95	-111.83	-112.86	-112.66	-112.28	-113.00	-112.93	-112.49
Deviance	225.76	225.62	222.56	225.43	225.33	225.96	224.71	224.29	226.13	225.99	224.97	224.85	225.68	225.91	223.66	225.72	225.32	224.56	226.01	225.85	224.97
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.33***	0.17	0.02	0.60***	−0.04	0.61***	0.28*	0.15	0.10	0.95***	−0.39*	−0.09	−0.37***	−0.17	0.15	0.13	−0.50***	−0.16	−0.47**	0.22*	−0.04
	(0.06)	(0.12)	(0.09)	(0.13)	(0.15)	(0.10)	(0.12)	(0.11)	(0.06)	(0.22)	(0.19)	(0.22)	(0.11)	(0.14)	(0.09)	(0.19)	(0.06)	(0.13)	(0.15)	(0.10)	(0.12)
DoS attack (t-1)	2.94***	2.97***	2.94***	2.74***	2.94***	2.88***	2.93***	2.92***	2.96***	2.84***	2.93***	2.95***	2.94***	2.96***	2.95***	2.92***	2.84***	2.94***	2.93***	2.90***	2.95***
	(0.37)	(0.39)	(0.39)	(0.31)	(0.39)	(0.34)	(0.40)	(0.40)	(0.38)	(0.35)	(0.39)	(0.37)	(0.37)	(0.37)	(0.40)	(0.41)	(0.39)	(0.39)	(0.40)	(0.36)	(0.39)
AIC	352.53	353.70	353.93	349.41	354.07	349.92	351.95	353.65	353.91	346.82	352.84	353.82	351.61	352.94	353.94	353.82	352.07	353.56	352.36	353.69	353.94
BIC	749.60	750.77	751.00	746.47	751.13	746.98	749.02	750.71	750.97	743.89	749.90	750.88	748.68	750.00	751.01	750.89	749.13	750.62	749.43	750.75	751.00
Log Likelihood	-112.27	-112.85	-112.97	-110.70	-113.03	-110.96	-111.98	-112.82	-112.95	-109.41	-112.42	-112.91	-111.81	-112.47	-112.97	-112.91	-112.03	-112.78	-112.18	-112.84	-112.97
Deviance	224.53	225.70	225.93	221.41	226.07	221.92	223.95	225.65	225.91	218.82	224.84	225.82	223.61	224.94	225.94	225.82	224.07	225.56	224.36	225.69	225.94
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.1.9: Penalized logistic regression results - medium-term models (newspaper and day fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

D.2 Topic Modeling

In this appendix, I present the results of the generated topics, when K is set to 50, 25 or 100. The main result with K=50 is shown in Table D.2.1. Table D.2.2 highlights that many of the terms correspond to mixed topics when I consider 25 topics (Table D.2.2), while for Table D.2.3 (K=100) it is difficult to distinguish between the topic as some of them are very similar.

p(z)	Label	Top words	Internal valid?
0.066324	General opinion	Venezuela:0.014451 country:0.010544 continue:0.007950 can:0.007115 Venezuelan:0.006993 politics:0.006879 will be:0.006266 should:0.006143 alone:0.005320 economy:0.005207 live:0.005056 make:0.004913 social:0.004655 Maduro:0.004530 could:0.004332	Yes
0.043895	Sanctions	Venezuela:0.045923 USA:0.023625 sanction:0.023301 United:0.022011 government:0.018773 embassy:0.014289 Venezuelan:0.014024 Maduro:0.012839 country:0.012811 European:0.012113 Union:0.009741 EU:0.008805 election:0.008598 reject:0.007592 officials:0.006909	Yes
0.041180	National assembly	national:0.053728 assembly:0.035471 dispute:0.024873 president:0.015611 AN:0.012692 politics:0.010413 Venezuela:0.009298 constituent:0.009128 Maduro:0.008510 government:0.007927 commission:0.007764 party:0.007629 ensure:0.007343 new:0.006602 ANC:0.006557	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.040474	Maduro	Maduro 0.089321 president:0.048436 Nicolas:0.044773 Venezuela:0.020501 government:0.014672 Venezuelan:0.014575 ensure:0.009381 announce:0.008243 national:0.008113 republic:0.007715 election:0.007357 country:0.006637 new:0.005980 presidential:0.005932 Santos:0.005134	Yes
0.039453	Opposition candidate	Falcon:0.026931 candidate:0.026306 presidential:0.026221 Henri:0.019067 election:0.017800 Maduro:0.011979 opposition:0.010491 vote:0.010328 candidacy:0.009921 party:0.009607 president:0.008389 electoral:0.008336 Venezuelan :0.008193 ensure:0.008181 government:0.007562	Yes
0.038004	Government-opposition dialog	dialog:0.038177 government:0.036453 opposition:0.026216 Venezuelan:0.019267 Dominican:0.016998 Venezuela:0.015758 Republic:0.014486 agreement:0.014191 president:0.012837 Jorge:0.010237 meeting:0.010039 chancellor:0.008789 Maduro:0.008696 Rodriguez:0.008525 national:0.008311	Yes
0.035994	Election	election:0.044032 electoral:0.041866 presidential:0.026213 CNE:0.021575 national:0.019208 council:0.016683 elections:0.010967 party:0.010370 vote:0.010189 process:0.009810 president:0.008820 next:0.007539 municipal:0.007472 realize:0.007101 Venezuela:0.007011	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.033783	Migration crisis	Venezuelan:0.062987 country:0.022501 Venezuela:0.018283 Colombia:0.015586 crisis:0.010881 international:0.007737 Brazil:0.007488 humanitarian:0.007452 border:0.007188 migration:0.006905 help:0.006682 thousands:0.006681 refugees:0.006124 national:0.005798 citizens:0.005518	Yes
0.031420	Protest / Shortages	protest:0.027537 San:0.015367 missing:0.010183 municipal:0.010159 city:0.008252 sector:0.007497 neighbor:0.007388 national:0.007379 new:0.007128 bolivar:0.006942 denounce:0.006803 street:0.006725 transport:0.006715 regional:0.006701 habitat:0.006276	Yes
0.031162	Oscar Perez	Perez:0.022184 Oscar:0.020064 kill:0.016213 body:0.011489 official:0.009250 steal:0.008872 police:0.008558 men:0.008435 two:0.008316 dead:0.007951 CICPC:0.007948 national:0.007672 dead:0.007656 year:0.006789 Venezuelan:0.006496	Yes (incl. other killings)
0.028106	Earthquake / accidents	dead:0.031197 hurt:0.025463 person:0.023265 at least:0.020505 leave:0.017647 two:0.013686 earthquake:0.012526 after:0.012195 international:0.011957 died:0.009862 magnitude:0.009730 accident:0.009463 result:0.008966 three:0.008569 registered:0.008514	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.027333	International Organizations	Venezuela:0.033977 rights:0.019264 international:0.018806 human:0.018235 denounce:0.012866 OAS:0.011484 UN:0.011290 general:0.011158 organisation:0.010889 government:0.010716 protest:0.009684 inform:0.009191 Almagro:0.008946 Nicaragua:0.008819 Luis:0.008695	Yes (focus on Nicaragua)
0.025594	Government ministers	minister:0.022420 Rodriguez:0.020474 national:0.015720 Cabello:0.013887 vicepresident:0.012889 social:0.012862 Venezuela:0.010987 plan:0.010562 party:0.009915 president:0.009407 Diosada:0.009055 ensure:0.008984 PSUV:0.007680 Lopez:0.007622 Jorge:0.007581	Mixed (not only ministers)
0.025438	Political Prisoners	prisoners:0.028654 political:0.026987 Penal:0.013729 liberty:0.013115 national:0.012490 arrest:0.012011 free:0.011634 Foro:0.011215 Venezuelan:0.009659 denounce:0.009321 director:0.007523 Helicoid:0.007405 SEBIN:0.007302 inform:0.006795 Romero:0.006385	Yes
0.024928	USA / Korea	Trump:0.051455 president:0.028576 Donald:0.025267 USA:0.019123 Korea:0.018888 United:0.018715 North:0.015156 US-American:0.013238 Kim:0.012052 Jong:0.009752Jerusalem:0.009233 China:0.008804 international:0.008607 summit:0.008452 announce:0.006899	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.024925	Petroleum	Venezuel:0.025539 petroleum:0.021110 production:0.016822 Venezuelan:0.014950 prize:0.014382 country:0.013712 economy:0.013455 million:0.013265 dollar:0.012994 year:0.012678 barrel:0.011584 inflacion:0.010082 OPEC:0.009600 according:0.009005 oil:0.008977	Yes
0.022507	Resignations	president:0.042073 America:0.023391 Peru:0.022901 summit:0.019598 Kuczynski:0.013540 Venezuela:0.012032 Lima:0.011251 resignation:0.010724 Chile:0.009862 Madur:0.009205 Pedro:0.009171 country:0.009132 Pablo:0.009053 congress:0.008785 after:0.007998	Yes
0.021977	Corruption	prosecution:0.024146 Saab:0.019186 general:0.018316 Rafael:0.014747 Tarek:0.014059 corruption:0.013842 Ramirez:0.013662 William:0.013165 PDVSA:0.011895 arrest:0.011211 republic:0.011018 house:0.010497 investigation:0.009558 president:0.009064 accuse:0.008794	Yes
0.020878	Salary / prices	Bolivar:0.025164 increase:0.023093 payment:0.021588 million:0.018980 transport:0.018087 salary:0.017085 bs:0.015475 pension:0.012852 thousand:0.012006 passanger:0.011831 minimum:0.010897 public:0.009525 work:0.008890 venezolan:0.008314 new:0.008118	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.019830	Colombia border	Colombia:0.044504 Colombian:0.019540 Venezuelan:0.014170 border:0.013419 Venezuela:0.012413 two:0.011176 Santos:0.010908 ELN:0.009826 kidnapping:0.009307 FARC:0.008024 Juan:0.007949 international:0.007826 peace:0.007581 national:0.007511 Manuel:0.007463	Yes
0.019772	Shortages healthcare	patient:0.026464 hospital:0.023871 health:0.020674 missing:0.018602 doctors:0.015288 medicines:0.013541 supplies:0.013279 protest:0.010530 medicine:0.009601 shortage:0.009472 work:0.009059 Venezuela:0.009036 denounce:0.008976 country:0.007416 crisis:0.007010	Yes
0.019346	Exchange rate	new:0.024480 bank:0.019940 monetary:0.019644 Dicom:0.018367 Venezuela:0.015966 change:0.015510 exchange:0.015453 auction:0.013899 bolivar:0.013158 BCV:0.013088 money0.012494 reconversion:0.011268 central:0.011134 dollar:0.010789 system:0.010561	Yes
0.019185	Shortages	Caracas:0.040046 metro:0.018553 water:0.018338 services:0.015670 national:0.012043 Vargas:0.008916 municipal:0.008800 station:0.008300 informe:0.007954 Miranda:0.007838 work:0.007480 hydrocapital:0.007179 transport:0.007008 failure:0.006609 santo:0.006578	Mostly (also includes advertising)

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.018979	Russia	Syria:0.027777 Russia:0.017495 attack:0.017285 international:0.015124 Russian:0.012889 Argentina:0.010564 United:0.008763 submarine:0.008446 Frace:0.008277 Putin:0.008244 president:0.007088 after:0.006721 USA:0.006439 chemical:0.006237 queen:0.005758	Mostly (includes miss world election)
0.018727	Outages	electricity:0.044275 Zulia:0.021333 failure:0.019987 service:0.016423 blackout:0.011093 Maracaibo:0.010084 Corpoelec:0.009591 inform:0.009560 affected:0.009134 sector:0.008918 Tachira:0.008877 Motta:0.008758 Dominguez:0.008650 energy:0.008320 minister:0.008070	Yes (including sabotage)
0.018245	Exiled opposition	Ledezma:0.040742 Antonio:0.027935 Venezuela:0.021408 Spain:0.018790 government0.014410 Spanish:0.014403 president:0.014013 metropolitan:0.013841 mayor:0.013214 Caracas:0.012902 Puigdemont:0.012514 Venezolan:0.011921 Carl:0.010896 international:0.010339 Maria:0.009350	Yes
0.018224	Music / entertainment	new:0.014320 Venezuelan:0.009153 prize:0.005712 present:0.005545 woman:0.005373 international:0.005192 world:0.005027 here:0.004939 know:0.004871 ano:0.004569 first:0.004397 music:0.004352 public:0.004266 first:0.004119 be:0.004115	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.017594	Child mortality	years:0.039488 children:0.028425 Venezuelan:0.021119 died:0.010578 mother:0.009790 death:0.009289 year:0.009221 two:0.008149 son:0.008137 deaths:0.008097 Jose:0.007089 after:0.007072 national:0.006506 baby:0.006401 then:0.006092	Mixed (not only child mortality)
0.017069	Court sentences	Lula:0.025963 court:0.018376 ex-president:0.016171 da:0.015788 Brazil:0.015525 justice:0.014857 Silva:0.014425 years:0.013726 sentence:0.013651 supreme:0.012469 prisoner:0.011982 Brazilian:0.011207 TSJ:0.009975 prison:0.009128 president:0.009089	Yes
0.015727	PDVSA	PDVSA:0.042174 Venezuela:0.031467 debt:0.023113 payment:0.020954 oil:0.017441 bond:0.016686 petroleum:0.011817 million:0.010063 state:0.008553 firm:0.008492 Venezuelan:0.007550 government:0.007102 dollar:0.006775 international:0.006668 Quevedo:0.006163	Yes
0.014823	Church / job offer (mixed)	Pope:0.038525 Francis:0.027935 holy:0.014790 search:0.014390 journalist:0.014237 community:0.012937 social:0.012187 digital:0.011932 Venezuela:0.010226 churchi:0.008999 celebrate:0.008560 Venezuela:0.008235 international:0.007716 Vatican:0.006471 like:0.006349	Mixed (only church)

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.014736	Food policy	food:0.017743 prize:0.013776 CLAP:0.012731 product:0.010879 production:0.010024 million:0.009108 thousand:0.009091 meat:0.008608 food 0.008527 buy:0.008381 deliver:0.008323 national:0.007934 kilo:0.006853 ton:0.006778 sell:0.006158	Mixed (includes recipes)
0.013925	Airline (opening/closing)	Venezuela:0.039317 airlin:0.024934 Venezuelan:0.018155 Panama:0.018075 flight:0.017685 open:0.017185 aounce:0.014610 Copa:0.014332 airline:0.012854 air:0.012139 Curaza:0.011048 country:0.010516 Aruba:0.010010 suspend:0.009868 end:0.009159	Yes
0.012826	Indigenous groups / diseases	Delta:0.023141 Amacur:0.019440 community:0.018882 boy:0.016134 indigenous:0.015425 Wara:0.014064 almost:0.013647 denounce:0.012809 Venezuela:0.010598 measle:0.009564 malnutrition:0.009221 missing:0.009012 health:0.008951 malaria:0.008236 affect:0.007555	Yes
0.012719	Education Studies	study:0.025545 universal:0.023648 national:0.012353 education:0.012114 profesor:0.010790 public:0.010599 University:0.010201 school:0.010072 institute:0.009981 schools:0.009835 educated:0.009735 class:0.006813 crisis:0.006421 year:0.006140 month:0.006062	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.011546	Mining / sport (mixed)	mining:0.019540 Venezuela:0.013718 Arco:0.012923 gold:0.012574 Venezuelan:0.011401 win:0.007119 world:0.007034 football:0.006970 two:0.006945 play:0.006856 final:0.006496 great:0.006403 Orinicoc:0.006385 years:0.005932 year:0.005729	Yes (mixed topic)
0.009951	Economy policy	Sundde:0.033807 prize:0.027698 secure:0.023546 personal:0.020700 debt:0.015170 national:0.013595 credit:0.013442 opinion:0.013152 superintendent:0.012685 finance:0.012598 trade:0.012375 will be:0.011353 financing:0.010902 import:0.010844 represent:0.010840	Yes
0.009760	Recession	economy:0.069400 income:0.037787 economy:0.032495 petroleum:0.028953 Venezuela:0.022918 problem:0.020949 product:0.020823 recession:0.020721 money:0.020089 less:0.019971 flow:0.019570 abroad:0.019566 continue:0.019026 import:0.018562 impact:0.017875	Yes
0.008951	Cryptomoney	Petro:0.056755 cryptomoney0.039489 market:0.033936 would change:0.024953 Venezuelan:0.024112 economic:0.019942 service:0.016793 permit:0.015340 dol:0.015023 exchange:0.014862 well:0.013810 exterior:0.013092 liberation:0.012853 it:0.012633 flow:0.011332	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.008886	Economy opinion	politics:0.044283 economy:0.041736 Venezuelan:0.029005 measurements:0.028426 crisis:0.028222 take:0.027625 economy:0.025953 necessary:0.023656 opportunity:0.022387 president:0.021933 governmental:0.021697 new:0.020312 deterioration:0.019154 ideal:0.019131 manage:0.018914	Yes
0.008552	Military	forces:0.024590 armed:0.024374 national:0.017667 account:0.016883 military:0.016291 Banesco:0.015305 Venezuela:0.014304 crisis:0.012803 intervencion:0.012259 official:0.012019 institution:0.011701 government:0.009945 also:0.009526 FANB:0.009493 barracks:0.009180	Mostly (includes some other headlines)
0.007179	Work opinion	work:0.041266 company:0.034561 benefits:0.031346 can:0.030131 Venezuelan:0.024452 open:0.022773 cost:0.020917 infrastructure:0.018911 result:0.016888 reduce:0.015983 better:0.015616 labor:0.015438 point:0.015352 well:0.014166 manage:0.014092	Yes (about distant work)
0.007131	Cuba	Diaz:0.043007 Cuba:0.036575Luis:0.035531 Castro:0.028181 Cuban:0.016626 Ortega:0.016372 president:0.016216 Raul:0.016193 channel:0.013845 Vicent:0.012640 children:0.011630 Miguel:0.011417 way:0.011174 Fidell:0.011105 Marquez:0.009449	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.005473	Weather	Inameh:0.062016 country:0.057035 national:0.046779 rain:0.039776 precipitate:0.037470 part:0.036974 great:0.035524 cloud:0.033585 weather:0.025155 forecast:0.022413 Venezuela:0.021691 dispersion:0.021248 after:0.020752 predict:0.018987 region:0.018153	Yes
0.005210	Leftist opposition	program:0.031889 oligarchy:0.024329 horror:0.024171 alone:0.018900 government:0.018821 pact:0.016619 fight:0.014528 saman:0.014252 electoral:0.014181 occupy:0.013920 towards:0.013589 direct:0.012989 control:0.012295 travel:0.011222 sentence:0.010827	Yes
0.004710	Regulations	law:0.117708 sport:0.083348 vem:0.046064 fond:0.045505 right:0.035748 embargo:0.028618 project:0.027029 treaty:0.026523 can:0.026305 organize:0.026287 company:0.025161 tax:0.024812 respect:0.024795 impose:0.024612 regulation:0.022936	Yes
0.004517	Investment / infrastructure	society:0.042481 Venezuela:0.034329 will be:0.033000 corporate:0.029470 every:0.029416 stay:0.029361 limited:0.022601 time:0.022328 Caracas:0.019580 pass:0.018725 office:0.018343 opinion:0.018224 square:0.017406 comunnity:0.017378 build:0.017333	Yes

Continue on the next page

p(z)	Label	Top words	Internal valid?
0.004514	Investment	group:0.068389 intention:0.054658 person:0.043887 service:0.042439 acquire:0.039626 condition:0.036157 achieve:0.035501 debt:0.035091 basic:0.034336 product:0.033880 a few:0.032050 certain:0.029710 meeting:0.028417 time:0.028390 finance:0.026633	Yes
0.004283	Spanish development aid	Spanish:0.081387 political:0.047098 achieve:0.044364 technical:0.041265 Miraflores:0.041063 organization:0.041006 last:0.040065 cystic:0.039154 similar:0.038712 could:0.038319 circle:0.038204 word:0.037091 opinion:0.036573 try:0.035057 result:0.032908	Yes
0.004234	Financial market	circulation:0.050091 ticket:0.046529 was:0.041919 Venezuelan:0.040599 total:0.040463 recent:0.039386 traditional:0.039299 oscillation:0.038318 liquidity:0.038027 quantity:0.037590 measurement:0.036901 continue:0.036765 descendent:0.036688 opinion:0.036290 yet:0.036018	Yes

Table D.2.1: Generated Topics (K=50). Note: Words are translated and unstemmed. $P(z)$ shows the distribution of the topics over the whole corpus of 123 574 headlines. Probabilities after words display the likelihood of a specific word appearing in the respective topic. Top 15 words for each topic are displayed. To further check the semantic validity, I investigated whether the top 30 headlines per category correspond to the identified topic (see last column and replication files).

p(z)	Label	Top words
0.079420	Maduro	madur:0.015353 venezuel:0.011715 gobiern:0.007832 venezolan:0.007441 si:0.007168 polit:0.006651 pais:0.006362 president:0.006061 sol:0.006018 nicol:0.005448
0.072853	National assembly	nacional:0.034377 asamble:0.021469 venezuel:0.020858 diput:0.014546 madur:0.012585 president:0.012233 gobiern:0.010190 venezolan:0.008637 derech:0.008179 luis:0.008086
0.072600	Election	eleccion:0.031827 presidencial:0.026818 electoral:0.024757 candidat:0.015666 falcon:0.013889 nacional:0.013662 part:0.011961 cne:0.011839 vot:0.010245 henri:0.009997
0.056434	Venezuela crisis	venezuel:0.022298 pais:0.018288 venezolan:0.017166 crisis:0.016369 social:0.008796 econom:0.008700 busc:0.007480 period:0.007145 nacional:0.006426 comun:0.006372
0.055839	Protest / shortages	protest:0.011668 nacional:0.010548 san:0.009214 municipi:0.007373 carac:0.006122 com:0.006047 falt:0.005786 denunci:0.005287 tachir:0.005255 clap:0.005213
0.054978	Political prisoners / corruption (mixed)	nacional:0.012884 pres:0.011297 deten:0.011021 general:0.010812 fiscal:0.010656 polit:0.010234 denunci:0.009013 saab:0.008222 penal:0.008128 inform:0.007873
0.053011	Government-opposition dialog	gobiern:0.031470 dialog:0.028227 venezuel:0.024858 oposicion:0.018906 venezolan:0.014016 dominican:0.012328 rodriguez:0.012235 acuerd:0.012049 republ:0.011602 president:0.011427

Continue on the next page

p(z)	Label	Top words
0.050881	Lima summit	madur:0.048480 president:0.048141 nicol:0.024117 venezuel:0.018958 amer:0.013052 cumbr:0.011171 peru:0.010864 pais:0.008163 nuev:0.007887 cub:0.007640
0.046849	International	trump:0.030378 unid:0.020193 eeuu:0.019987 president:0.017360 donald:0.014716 internacional:0.010707 core:0.010330 siri:0.009236 estadounidens:0.008925 rusi:0.008639
0.046246	Electricty / transportation (mixed)	electr:0.019691 carac:0.017878 servici:0.015214 transport:0.014657 trabaj:0.013992 fall:0.011721 nacional:0.010044 agu:0.009924 zuli:0.008331 inform:0.007629
0.045831	Cryptomoney	venezuel:0.017274 millon:0.015026 banc:0.013845 pag:0.012227 petr:0.012055 bolivar:0.010272 ser:0.009946 nuev:0.009860 dolar:0.009414 criptomoned:0.009399
0.042986	Oscar Perez / crime (mixed)	anos:0.018961 asesin:0.014375 perez:0.014209 oscar:0.012655 venezolan:0.011470 dos:0.010226 muert:0.008305 cuerp:0.007612 nin:0.007411
0.042433	Border colombia / airline (mixed)	venezolan:0.041813 venezuel:0.029001 colombi:0.025387 pais:0.012944 fronter:0.008809 colombian:0.008618 internacional:0.008599 airlin:0.008195 oper:0.007977 sant:0.007390
0.040694	Entertainment / sport	venezolan:0.012949 nuev:0.007546 venezuel:0.007257 anos:0.006350 ano:0.006221 mund:0.005819 dia:0.005572 celebr:0.004839 premi:0.004595 internacional:0.004187

Continue on the next page

p(z)	Label	Top words
0.039588	Accident / crime	muert:0.027149 person:0.020144 her:0.019255 men:0.018134 dej:0.014590 internacional:0.012456 dos:0.011956 tras:0.011412 ataqu:0.009300 mur:0.008952
0.034902	Sanctions / Exiled opposition	venezuel:0.035857 venezolan:0.025098 sancion:0.024881 polit:0.020451 ledezm:0.017487 gobiern:0.016127 madur:0.014967 eeuu:0.014627 unid:0.014545 med:0.013407
0.031581	Petroleum / PDVSA	economi:0.024733 pdvsa:0.023938 petrole:0.021327 venezuel:0.020809 petroler:0.018159 econom:0.017750 produccion:0.016063 venezolan:0.012232 millon:0.010307 dolar:0.010142
0.030265	Healthcare / indigenous groups (mixed)	pacient:0.017276 hospital:0.016628 falt:0.014856 salud:0.014053 medic:0.010417 denunci:0.010216 nin:0.009707 delt:0.009145 medicament:0.008791 protest:0.008239
0.027576	Court sentences	lul:0.016735 expresident:0.013682 president:0.013223 tribunal:0.011833 justici:0.011018 brasil:0.010788 da:0.010680 internacional:0.010241 silv:0.009785 puigdemont:0.009403
0.020850	Prices	economi:0.031018 preci:0.026914 product:0.020256 moned:0.015374 fluj:0.014106 aument:0.013981 merc:0.013454 salari:0.013424 sundd:0.013363 ingres:0.013197
0.014110	Church / Sport (mixed)	ley:0.035633 pap:0.035589 deport:0.028841 francisc:0.025013 vem:0.015481 derech:0.014921 fond:0.014608 venezuel:0.011986 trat:0.010121 embarg:0.009946

Continue on the next page

p(z)	Label	Top words
0.013142	Financial opinion	deb:0.026109 pued:0.024622 grup:0.024117 product:0.020311 intencion:0.019462 servici:0.019393 person:0.018366 finanz:0.017752 segur:0.017395 cumpl:0.017285
0.012554	Weather / Earthquake (mixed)	pais:0.029430 inameh:0.027056 sism:0.024840 nacional:0.023426 lluvi:0.020678 magnitud:0.019721 part:0.017504 venezuel:0.017271 gran:0.016648 precipit:0.016415
0.009417	Inflation	billet:0.036833 circulacion:0.028586 venezolan:0.025601 hiperinflacion:0.023447 habi:0.021934 total:0.020851 recient:0.020536 monetari:0.020108 aun:0.019430 sig:0.018731
0.004961	Financial market	espanol:0.075121 polit:0.046258 organizacion:0.039371 logr:0.038758 ultim:0.037258 tecnic:0.037250 pod:0.035750 miraflor:0.035750 parec:0.034822 palabr:0.034615

Table D.2.2: Generated Topics (K=25). Note: Words are not translated and only stems are displayed. $P(z)$ shows the distribution of the topics over the whole corpus of 123 574 headlines. Probabilities after words display the likelihood of a specific word appearing in the respective topic. Top 10 words for each topic are displayed.

p(z)	Label	Top words
0.039521	Venezuela	venezuel:0.011246 pais:0.009467 polit:0.008965 madur:0.008425 ser:0.006103 venezolan:0.005884 si:0.005500 pas:0.005333 pod:0.005256 anos:0.005061
0.039510	Crisis economy	venezuel:0.024993 venezolan:0.017998 madur:0.016847 asegur:0.015867 pais:0.015593 gobiern:0.014904 deb:0.010713 polit:0.010574 president:0.010235 nacional:0.008999
0.027087	Election	eleccion:0.063479 presidencial:0.042912 venezuel:0.025052 electoral:0.019293 vot:0.015919 madur:0.014580 president:0.013670 comici:0.012022 venezolan:0.011346 proxim:0.010210
0.025517	Maduro	madur:0.112147 president:0.063265 nicol:0.058887 gobiern:0.015828 anunci:0.013820 venezuel:0.013817 republ:0.013465 venezolan:0.013005 nacional:0.011495 nuev:0.010287
0.024949	National assembly	nacional:0.070420 asamble:0.050943 diput:0.034085 president:0.019754 an:0.018184 constituyent:0.012861 comision:0.011987 polit:0.009855 anc:0.009600 nuev:0.009036
0.023068	Sanctions	sancion:0.041392 venezuel:0.034480 gobiern:0.030520 eeuu:0.026573 unid:0.024340 venezolan:0.019695 europe:0.018256 union:0.014794 madur:0.013463 ue:0.012964
0.022643	Migration crisis	venezolan:0.082273 colombi:0.019235 pais:0.019217 brasil:0.010298 mil:0.009712 venezuel:0.009115 migracion:0.008053 fronter:0.007928 refugi:0.007731 migrant:0.007457

Continue on the next page

p(z)	Label	Top words
0.019803	Opposition candidates	falcon:0.050927 henri:0.036621 presidencial:0.033537 candidat:0.032173 candidatur:0.017465 madur:0.017228 eleccion:0.013922 electoral:0.012042 part:0.011275 oposicion:0.009925
0.019589	Government-opposition dialog	dialog:0.058814 gobiern:0.048190 oposicion:0.040616 dominican:0.030076 republ:0.021649 acuerd:0.016642 venezolan:0.016009 mes:0.014300 negociacion:0.011706 reunion:0.011555
0.018125	Election	electoral:0.056043 cne:0.037798 nacional:0.030492 consej:0.027514 eleccion:0.025455 part:0.015853 presidencial:0.012211 proces:0.012029 rector:0.010048 municipal:0.009989
0.017358	Accidents / deaths	muert:0.040736 her:0.032104 person:0.031024 men:0.025398 dej:0.024484 accident:0.015471 tras:0.015079 dos:0.014161 internacional:0.012508 result:0.011303
0.017170	Government ministers / meetings	venezuel:0.048255 ministr:0.020004 cancill:0.018796 pais:0.018654 arreaz:0.017493 relacion:0.016820 exterior:0.013371 jorg:0.013170 president:0.012338 reunion:0.011156
0.017159	Security Forces	funcionari:0.020229 deten:0.017995 nacional:0.017241 dos:0.016821 polici:0.015998 presunt:0.011103 bolivarian:0.011048 rob:0.010004 tres:0.009003 gnb:0.008322
0.016973	Lima summit	amer:0.041863 venezuel:0.038382 cumbr:0.034537 madur:0.025896 president:0.023184 lim:0.019703 peru:0.018553 pais:0.013844 eeuu:0.010189 grup:0.009684

Continue on the next page

p(z)	Label	Top words
0.016819	Inflation	venezuel:0.028376 econom:0.026383 economi:0.020831 ano:0.019394 inflacion:0.017886 pais:0.012255 segun:0.011650 crisis:0.010703 indic:0.010603 preci:0.008803
0.016546	Political prisoners	polit:0.036993 pres:0.036077 penal:0.019577 for:0.016874 liber:0.015498 libert:0.013171 denunci:0.012552 nacional:0.012519 deten:0.011925 venezolan:0.010120
0.016196	Protest / shortages	protest:0.040749 agu:0.020930 san:0.020351 falt:0.014297 vecin:0.013789 habit:0.012142 sector:0.010995 municipi:0.010962 servici:0.009948 exig:0.009635
0.015207	Shortages	electr:0.055677 fall:0.024223 servici:0.024055 agu:0.017029 zuli:0.016079 carac:0.013916 apagon:0.013534 sistem:0.011804 inform:0.011782 corpoelec:0.011344
0.015075	Crisis	venezuel:0.037642 crisis:0.034431 pais:0.028876 venezolan:0.022676 humanitari:0.018408 situacion:0.016924 econom:0.012995 salud:0.011427 emergent:0.010455 internacional:0.007950
0.014888	Crime / deaths	asesin:0.028809 anos:0.024711 venezolan:0.018506 hombr:0.013348 mat:0.012613 jov:0.010511 muj:0.010044 hall:0.009928 dos:0.009350 rob:0.008266
0.014071	Shortages healthcare	pacient:0.035797 hospital:0.030630 falt:0.023351 medic:0.020176 insum:0.017836 salud:0.017207 medicament:0.015568 protest:0.013936 medicin:0.011534 denunci:0.011010

Continue on the next page

p(z)	Label	Top words
0.013895	USA / Korea	trump:0.065755 donald:0.033339 core:0.032521 president:0.032067 nort:0.025294 kim:0.021528 jong:0.017466 unid:0.016693 estadounidens:0.015055 eeuu:0.013846
0.013514	Exiled opposition	ledezm:0.061761 antoni:0.043044 venezuel:0.026591 carac:0.021391 metropolitan:0.019856 venezolan:0.018610 alcald:0.017413 madur:0.014400 espan:0.013081 gobiern:0.011335
0.013264	Colombian politics	colombi:0.065391 colombian:0.029758 sant:0.022480 venezuel:0.019069 fronter:0.016881 eln:0.015251 president:0.014302 farc:0.012983 paz:0.011723 manuel:0.011583
0.012132	Protest	ciud:0.016612 centr:0.016073 boliv:0.013453 saque:0.013243 report:0.011350 protest:0.009080 puert:0.008981 tras:0.008683 person:0.007750 regional:0.007611
0.011973	Cryptomoney	petr:0.035583 dicom:0.029171 criptomoned:0.026084 divis:0.025836 subast:0.024052 dolar:0.020102 cambi:0.019799 dol:0.015464 bolivar:0.013659 tas:0.013112
0.011825	International organizations	derech:0.043942 venezuel:0.037971 human:0.032367 onu:0.029039 internacional:0.023859 comision:0.016747 organizacion:0.011296 cidh:0.011129 nacion:0.010732 unid:0.010683
0.011661	Regional organizations	luis:0.036148 orteg:0.036145 diaz:0.025146 general:0.024115 oea:0.022763 venezuel:0.022301 madur:0.020780 almagr:0.020769 internacional:0.017310 nicaragu:0.016350

Continue on the next page

p(z)	Label	Top words
0.011196	Corruption	fiscal:0.043043 saab:0.040293 general:0.030793 tarek:0.029433 william:0.027404 republ:0.018959 deten:0.013103 nacional:0.011525 inform:0.011158 corrupcion:0.010959
0.010905	Transportation	transport:0.071232 public:0.024469 pasaj:0.023680 aument:0.012070 carac:0.011836 falt:0.009655 unidad:0.008953 servici:0.008383 par:0.008073 maracaib:0.008058
0.010796	Airline (opening / closeing)	venezuel:0.043501 airlin:0.031911 vuel:0.021430 panam:0.020527 venezolan:0.020508 oper:0.019966 cop:0.018174 anunci:0.016135 aeroline:0.016051 aere:0.014953
0.010796	Petroleum production	petrole:0.046322 produccion:0.029486 barril:0.026257 dolar:0.025834 venezuel:0.025437 opep:0.022189 millon:0.019928 venezolan:0.018274 crud:0.018266 petroler:0.015563
0.010693	Protest / education	trabaj:0.048218 nacional:0.014950 colegi:0.011082 pag:0.010928 educacion:0.010727 protest:0.010516 anunci:0.009773 educ:0.009673 institu:0.009500 exig:0.008980
0.010355	Oscar Perez	perez:0.071974 oscar:0.068265 cuerp:0.020557 junquit:0.016622 cicpc:0.011352 familiar:0.010982 oper:0.010167 investig:0.010072 nacional:0.009861 ex:0.009313
0.009982	Russia	siri:0.028676 president:0.024078 eeuu:0.017511 unid:0.017230 rusi:0.015878 iran:0.013688 internacional:0.013396 putin:0.013322 acuerd:0.012922 franci:0.012860

Continue on the next page

p(z)	Label	Top words
0.009941	Child mortality	nin:0.061709 anos:0.033434 desnutricion:0.013310 edad:0.011592 beb:0.011430 muri:0.010569 muert:0.010482 falleci:0.010449 hospital:0.010412 madr:0.010105
0.009915	Resignations	president:0.031834 peru:0.029464 kuczynski:0.027455 tribunal:0.024258 tsj:0.022474 pedr:0.018991 suprem:0.018248 pabl:0.018223 justici:0.018202 renunci:0.015583
0.009596	Music / Royal wedding	venezolan:0.016000 premi:0.013093 nuev:0.010528 internacional:0.009465 princip:0.008495 anos:0.007895 megh:0.006385 music:0.006313 present:0.005849 asi:0.005584
0.009569	Municipal candidates	candidat:0.026760 alcaldi:0.026441 municipi:0.026007 alcald:0.018214 social:0.013096 carac:0.011956 barut:0.010559 libert:0.010408 gomez:0.010352 gobern:0.010038
0.009553	Salary	bolivar:0.045225 millon:0.040482 aument:0.038436 salari:0.034011 bs:0.029510 minim:0.024452 mil:0.019084 preci:0.018395 canast:0.013424 madur:0.011089
0.009549	Lula da Silva	lul:0.047289 brasil:0.029670 da:0.028545 silv:0.026321 expresident:0.024144 brasilen:0.019498 prision:0.016279 inaci:0.015693 luiz:0.015343 conden:0.014180
0.009545	Opposition Frente Ample	frent:0.025002 gobiern:0.022010 popul:0.021489 ampli:0.020661 oposicion:0.020273 luch:0.019604 eleccion:0.018393 venezuel:0.014875 movimient:0.012650 particip:0.012568

Continue on the next page

p(z)	Label	Top words
0.009374	Puigdemot / Mugabe (mixed)	president:0.037797 puigdemont:0.028187 espanol:0.020189 gobiern:0.019201 espan:0.018025 mugab:0.017669 zimbabu:0.016598 carl:0.016128 independent:0.014732 catal:0.014513
0.009211	Military	lopez:0.027120 ministr:0.024113 padrin:0.018957 milit:0.018479 nacional:0.018104 defens:0.017389 militar:0.016755 fuerz:0.015664 armad:0.014869 reverol:0.011340
0.009098	Church	pap:0.067079 francisc:0.047852 sant:0.013270 iglesi:0.013175 vatican:0.011194 obisp:0.010240 chil:0.009987 internacional:0.009566 venezolan:0.009530 pid:0.009286
0.008654	Syria	ataqu:0.039876 siri:0.030528 muert:0.021759 atent:0.020309 men:0.017670 internacional:0.014579 bombarde:0.013600 mur:0.013447 grup:0.012140 terror:0.011693
0.008591	Bonuses / licenses	banc:0.030396 patri:0.017746 carnet:0.014269 pag:0.013584 nuev:0.011448 venezuel:0.010825 bon:0.010159 sistem:0.009757 document:0.009647 cit:0.009393
0.008527	Corruption	rafael:0.039066 ramirez:0.038115 corrupcion:0.023210 pdvsa:0.017849 odebrecht:0.014182 cas:0.013598 venezuel:0.012864 andorr:0.011827 investig:0.008864 ex:0.008859
0.008488	Sport	venezolan:0.016303 final:0.010718 gan:0.009594 jueg:0.009235 venezuel:0.009109 futbol:0.008643 mundial:0.008571 segund:0.008202 madr:0.007674 lig:0.006069

Continue on the next page

p(z)	Label	Top words
0.008128	Women / birth	si:0.014047 muj:0.012290 pued:0.010539 hac:0.010296 person:0.009218 deb:0.008454 sol:0.006145 eme:0.006019 sangr:0.005538 mejor:0.005361
0.008102	Exchange rate	monetari:0.047876 nuev:0.045784 reconversion:0.029382 billet:0.026447 moned:0.022928 con:0.019398 boliv:0.019073 anunci:0.013213 bcv:0.012970 president:0.012761
0.008045	South-Latin America	argentin:0.047878 president:0.027194 chil:0.024571 submarin:0.021717 juan:0.017236 piner:0.016679 hondur:0.016536 macri:0.013400 internacional:0.011283 san:0.011094
0.007800	Tourism	varg:0.017407 segur:0.015207 nacional:0.012095 activ:0.011314 pais:0.011188 sant:0.011061 turist:0.010813 carnaval:0.010449 mar:0.009880 civil:0.008571
0.007539	Pension	pension:0.034534 pag:0.024673 col:0.019794 efect:0.017824 cobr:0.017611 gasolin:0.016563 tachir:0.015761 banc:0.012978 bancari:0.011695 sudeb:0.011166
0.007501	Government announcment	rodriguez:0.088261 jorg:0.033296 ministr:0.023303 torr:0.018378 delcy:0.018219 nacional:0.015675 venezuel:0.014265 miguel:0.014090 president:0.013048 gobiern:0.011128
0.007388	Petroleum	pdvsa:0.073377 petroler:0.027401 empres:0.022523 petrole:0.022406 queved:0.014672 gas:0.013096 millon:0.012517 industri:0.012334 conocophillips:0.011170 venezuel:0.010490

Continue on the next page

p(z)	Label	Top words
0.007360	Internet	red:0.024941 social:0.018765 empres:0.010565 public:0.010375 usuari:0.010134 cuent:0.009665 criptomoned:0.009206 trav:0.009162 person:0.007764 telecomun:0.007306
0.007289	Prices	preci:0.022147 compr:0.021464 com:0.014042 product:0.013010 carn:0.011452 venezolan:0.010250 vid:0.008980 efect:0.008472 caf:0.008381 hiperinflacion:0.007682
0.007228	Government ministers	cabell:0.063287 vicepresident:0.048255 diosd:0.042296 part:0.024304 psuv:0.023667 unid:0.021361 prim:0.019233 social:0.017525 aissami:0.015721 venezuel:0.013985
0.007180	Prices	sundd:0.048453 preci:0.046854 comerci:0.018975 nacional:0.018758 supermerc:0.014467 superintendent:0.014272 product:0.013653 orden:0.012438 derech:0.012393 defens:0.012238
0.007120	School massacers/Trump (mixed)	escuel:0.027226 flor:0.025805 tirote:0.023707 eeuu:0.017750 nuev:0.013631 sexual:0.011897 miami:0.011331 york:0.010268 venezolan:0.009280 estudi:0.009112
0.007020	Israeli embassy	jerusal:0.039353 embaj:0.026655 israel:0.026251 palestin:0.022208 eeuu:0.021927 trump:0.019682 unid:0.019085 capital:0.018417 reconoc:0.016325 israeli:0.013923
0.006963	CLAP	clap:0.028395 produccion:0.026031 aliment:0.024448 entreg:0.014971 tonel:0.014162 nacional:0.012992 millon:0.011875 bernal:0.011149 freddy:0.011072 gobiern:0.010960

Continue on the next page

p(z)	Label	Top words
0.006609	Police	carabob:0.029581 motin:0.018074 policarabob:0.017370 carcel:0.015254 pres:0.014732 muert:0.014532 penitenciari:0.012510 comand:0.011993 lacav:0.011383 polici:0.010661
0.006526	Christmas	navid:0.026825 celebr:0.014856 tambi:0.012341 nin:0.011579 dia:0.011446 madr:0.011377 tradicion:0.010747 naviden:0.010431 venezolan:0.009436 regal:0.009360
0.006276	Recession	economi:0.059044 ingres:0.033189 product:0.032415 petroler:0.032022 problem:0.031767 recesion:0.031701 moned:0.030633 menor:0.030626 extranjer:0.030357 venezuel:0.030272
0.006250	Government	juan:0.043546 president:0.023613 pabl:0.022869 conindustri:0.017775 capril:0.015722 carl:0.014478 gobiern:0.012458 guanip:0.011602 olalquiag:0.010707 gremi:0.009904
0.006156	Education system	univers:0.046346 estudi:0.045464 universitari:0.018794 profesor:0.014424 nacional:0.013449 public:0.012360 cientif:0.012193 fundacion:0.011785 internacional:0.011317 relev:0.009995
0.006124	Indigenous groups	delt:0.050959 amacur:0.042873 wara:0.029610 comun:0.027964 denunci:0.022276 indigen:0.017186 falt:0.016185 tucupit:0.014788 municipi:0.012753 sarampion:0.010618
0.005961	Bonus payments	deud:0.052211 pag:0.039248 bon:0.038986 venezuel:0.038365 pdvsa:0.026830 default:0.014812 incumpl:0.012646 amp:0.012391 millon:0.011639 calificacion:0.011369

Continue on the next page

p(z)	Label	Top words
0.005951	Joshua Holt	venezuel:0.037401 eeuu:0.031658 holt:0.027587 estadounidens:0.024789 joshu:0.021057 unid:0.020967 marc:0.020684 rubi:0.019841 senador:0.017249 trump:0.014485
0.005878	Drug trade	anos:0.030671 cocain:0.023570 trafic:0.021716 dos:0.017672 conden:0.015874 flor:0.015224 venezuel:0.014902 drog:0.014384 sobrin:0.014230 unid:0.013740
0.005389	Cuba	cub:0.050715 castr:0.041002 diaz:0.024438 raul:0.021890 anos:0.020059 canel:0.017961 president:0.016763 fidel:0.016152 cuban:0.014993 miguel:0.012414
0.005132	Opposition campaigns / holidays (mixed)	pastor:0.020349 divin:0.013692 sant:0.013083 sam:0.012490 campan:0.012113 javi:0.011857 bertucci:0.011753 carac:0.011601 dia:0.010896 realiz:0.009085
0.004934	Mining	miner:0.055085 arco:0.035499 orinoc:0.021611 venezuel:0.020936 oro:0.019453 sur:0.014479 gobiern:0.014305 reserv:0.012605 recurs:0.012113 conoc:0.011297
0.004918	Diseases	cas:0.031026 palud:0.020770 salud:0.020528 sierr:0.017945 indigen:0.017001 perij:0.016257 venezuel:0.014151 comun:0.013958 malari:0.012738 brot:0.012646
0.004916	Earthquake	sism:0.073383 magnitud:0.056492 registr:0.032870 sacud:0.020093 sacudi:0.017618 terremot:0.016615 inform:0.013638 internacional:0.013580 funvisis:0.013295 escal:0.013111

Continue on the next page

p(z)	Label	Top words
0.004762	Weather	inameh:0.071270 pais:0.062034 nacional:0.046377 lluvi:0.043891 precipit:0.042268 part:0.040645 gran:0.038306 nub:0.037978 tiemp:0.028069 prev:0.024988
0.004752	Job offer	period:0.078783 busc:0.049933 social:0.045374 comun:0.038462 digital:0.037173 si:0.021921 gust:0.020061 trabaj:0.018072 venezuel:0.017734 globovision:0.017535
0.004659	Interview	chavez:0.023916 entrev:0.021040 pin:0.016559 hug:0.016276 viv:0.015862 president:0.015103 anos:0.014891 martinez:0.014794 eulogi:0.013824 nacional:0.012659
0.004597	Financial products	grup:0.058372 intencion:0.051693 cumpl:0.043073 person:0.034569 deb:0.034399 servici:0.034310 condicion:0.033514 vez:0.032307 basic:0.032253 merc:0.031753
0.004509	Caracas metro	carac:0.084729 metr:0.074311 estan:0.023807 oficin:0.023379 municipi:0.022850 chaca:0.022705 estacion:0.022048 opinion:0.019250 constru:0.018548 merced:0.018548
0.004422	Opposition	jos:0.044893 luis:0.034613 vicent:0.032633 ram:0.026062 leon:0.023125 allup:0.022112 president:0.018636 general:0.014416 democrat:0.013226 velasquez:0.012920
0.004383	Politics / economy opinion	polit:0.069490 tom:0.045392 econom:0.042936 oportun:0.042795 med:0.042167 gubernamental:0.039335 ideal:0.038294 desperdici:0.037535 economi:0.037010 venezolan:0.036897

Continue on the next page

p(z)	Label	Top words
0.004357	Russia - Great Britain	rus:0.054262 rusi:0.036445 diplomat:0.022561 exespi:0.017355 britan:0.016921 envenen:0.016761 skripal:0.015544 putin:0.013997 mar:0.013969 unid:0.013629
0.004285	Military intervention	banesc:0.043987 venezuel:0.031905 banc:0.023984 president:0.023821 lorenz:0.020263 mendoz:0.019975 intervencion:0.018402 escotet:0.013349 carl:0.013119 direct:0.011450
0.004006	Business opening	pued:0.049812 benefici:0.045208 trabaj:0.039567 cost:0.032131 infraestructur:0.031855 oper:0.031260 empres:0.029393 reduc:0.029014 venezuel:0.028768 result:0.027824
0.003760	Spanish development aid	espanol:0.089523 polit:0.049619 logr:0.049072 tecnic:0.046406 miraflor:0.045947 organizacion:0.044658 enquist:0.043926 parec:0.043762 corrill:0.043511 ultim:0.043227
0.003740	?	mari:0.047294 venezuel:0.034389 mach:0.031258 corin:0.028820 coordin:0.023932 vent:0.019363 public:0.018056 internacional:0.011543 necesit:0.009896 nacional:0.009479
0.003608	Regulations	ley:0.135799 deport:0.105959 vem:0.059998 fond:0.051266 derech:0.040200 embarg:0.033563 trat:0.031957 respect:0.030079 impon:0.029703 organ:0.029396
0.003532	Venezuela - Ecuador	ecuador:0.029007 asi:0.017597 especial:0.017574 capac:0.017423 hac:0.015783 corre:0.014783 peligr:0.013910 venezolan:0.013875 part:0.013457 lent:0.013457

Continue on the next page

p(z)	Label	Top words
0.003250	Inflation	billet:0.054713 circulacion:0.051555 total:0.050961 habi:0.050898 tradicional:0.049850 oscil:0.049471 liquidez:0.049041 recient:0.048536 cantid:0.047854 medicion:0.047841
0.003158	Exchange rate	economi:0.087529 merc:0.065191 cambiari:0.061031 venezolan:0.035898 intercambi:0.032570 bien:0.031738 permit:0.031348 fluj:0.030867 dol:0.030256 liberacion:0.030073
0.003136	Society	venezuel:0.067945 sociedad:0.060823 ser:0.050088 corpor:0.042770 pas:0.032755 comandit:0.032519 vez:0.031223 cad:0.029835 comun:0.027531 firm:0.025869
0.002753	Oligarchy opinion	program:0.050508 horror:0.045887 oligarqui:0.045663 pact:0.031635 ocup:0.031024 sol:0.029354 cuartel:0.024017 haci:0.023257 electoral:0.023212 direct:0.021989
0.002672	Expulsion ambassadors	embaj:0.062819 venezuel:0.037707 negoci:0.028891 encarg:0.028046 nuev:0.027001 grat:0.024713 miniaturiz:0.023223 inalambr:0.022639 marcapas:0.021933 robinson:0.021395
0.002633	Financial market products	segur:0.089919 ser:0.052883 deb:0.045700 personal:0.036741 import:0.035541 proteccion:0.034559 utiliz:0.032752 inteligent:0.032191 financ:0.031817 finanz:0.031521
0.002541	Petroleum export	ingres:0.067402 economi:0.043460 sensatez:0.043331 divis:0.037438 export:0.036873 represent:0.035646 petroler:0.034597 hidrocarbur:0.033693 asoci:0.033047 aproxim:0.032208

Continue on the next page

p(z)	Label	Top words
0.002511	Military	armad:0.039584 fuerz:0.039323 cuent:0.033278 crisis:0.029423 institucion:0.026596 nacional:0.021712 oficial:0.021074 cuartel:0.020062 fanb:0.019882 solicitud:0.019653
0.002420	?	llev:0.036435 dia:0.033757 cad:0.030114 cab:0.029283 estan:0.026131 riesg:0.020386 centr:0.020370 men:0.020031 especi:0.019844 sol:0.018065

Table D.2.3: Generated Topics (K=100). Note: Words are not translated and only stems are displayed. $P(z)$ shows the distribution of the topics over the whole corpus of 123 574 headlines. Probabilities after words display the likelihood of a specific word appearing in the respective topic. Top 10 words for each topic are displayed.

D.3 Categorization of Topics

In this appendix, I lay out in greater detail how I categorized the topics to broader categories. I undertook this step to ease the interpretation of the study's results. To this end, I qualitatively sorted the topics, orientating myself on the generated topics, newspaper categories in Venezuela and previous literature (e.g., King, Pan and Roberts, 2013; Tucker, 2007; Rozenas and Stukal, 2019; Walker, Rogers and Zelditch Jr, 1988). The broader categories are about the social/economic crisis in Venezuela, regime legitimacy, government-related issues, protests and repression, election related and international issues as well as one residual category ("other"), which includes non-political topics. Nevertheless, my categorization is not necessarily exclusive and topics may fall into multiple categories.

Category	P(z)	Topics
Social/economic crisis	0.272	Migration crisis, petroleum, salary/prices, shortages healthcare, exchange rate, shortages, outages, child mortality, PDVSA, airline (opening/closing), [indigenous groups/diseases], mining/sport (mixed), [recession], [economy opinion], work opinion, [investment/infrastructure], [investment], [Spanish development aid], [financial market]
Legitimacy	0.197	Sanctions, national assembly, international organizations, court sentences, resignations, corruption, exiled opposition, [leftist opposition]
Other	0.146	General opinion, education studies, music/entertainment, weather, earthquake/accidents, church/job offer (mixed)
Government	0.142	Maduro, government-opposition dialog, government ministers, food policy, economy policy, cryptomoney, regulations
Protest/repression	0.097	Protest/shortages, Oscar Perez, political prisoners, military
Election	0.075	Election, opposition candidate
International	0.071	Russia, Colombia border, USA/Korea, Cuba

Table D.3.1: Categorization of topics. Note: P(z) = distribution over whole corpus. Highly collinear topics are not included in the main analysis (within square brackets).

Table D.3.1 again summarizes the categorized topics. Whereas the categorization for most of the topics is straightforward, e.g., in the category social and economic crisis, all topics are primarily about the bad economy and social grievances, and the international, election-related, and protest/repression categories are self-explanatory, it is worthwhile to explain the topics within the legitimacy and government categories in greater detail.

All included topics in the legitimacy category question the legitimacy of the government, either internationally (sanctions, international organizations, exiled opposition) or domestically (the opposition filled national assembly, leftist opposition, court sentences, corruption). In theory, the international topics could also fall in the international category. Nevertheless, I believe that the legitimacy category is more informative as previous literature highlights that eroding levels of legitimacy may be dangerous for governments in power, therefore perceived as sensitive news by the government (cf. Walker, Rogers

and Zelditch Jr, 1988).

Concerning the government-related category, here, mainly government policies are included. However, the category also includes the broader topics *Maduro* and *government ministers*, which are also related to questions of legitimacy and/or election-related issues.

D.4 Robustness and Sensitivity Tests

In this appendix, I present the results of the robustness and sensitivity tests. The results of the robustness tests are again displayed graphically. This time the average marginal effects for all significantly related topics ($p < 0.05$) to the likelihood of DoS attacks are not ordered along broader categories to safe space. The complete results can be found in the Tables D.4.1 – D.4.52.

First, it could be that the found differences in the short- and medium-term models are due to the chosen lag lengths. Thus, I run short-term models considering t and t-1, as well as a comparable medium-term model that considers topic development for t-2 – t-7. Furthermore, in another analysis I expand the medium-term model to 14 days. The first two models (Figure D.4.1 [short-term] and Figure D.4.2 [medium-term]) show similar results as in the main analysis. Only the topics *Maduro*, *USA/Korea* and *resignations* appear now in both models.[1] Concerning the medium-term models that look at previous reporting up to 14 days before, Figure D.4.3 highlights indeed that more topics are overlapping. In addition to the topic *healthcare shortages*, now some topics are to a lesser (*election* and *exiled opposition*, *Cuba*) or higher (*protest/shortages*) degree related to the likelihood of attacks.[2] Due to the fact that the marginal effect of the topic *exiled opposition* is still twice as big in the medium-term models, I would still argue that this speaks more for the use of direct censoring for this topic, yet, the only clearly significant topics in the short-term model remain the *resignations*, *PDVSA* and *petroleum* topics.

Second, there might be the concern that the measured DoS attacks are not due to external interference but the general interest that causes a website to collapse (because of too many clicks). To investigate whether this is the case, I include a variable for each news outlet that should measure the general interest for the respective website. For this I use the R package *gtrendsR*, which is an API to Google Trends, and as search terms the respective newspaper names. Then, I retrieve the Google trend for the period of study for every website separately. The trend is a measure from 0 (no interest) to 100 (high interest) at a daily resolution relative to the point with the highest interest (and to the overall search queries). I lagged this variable by one day as DoS attacks may de- or increase the interest for specific websites. The marginal effect plots show quite similar results (see Figures D.4.4 and D.4.5).[3]

Third, I investigate which topics are negatively related to the likelihood of DoS attacks

[1] In addition, the topic *weather* is significantly correlated to the likelihood of DoS attacks in the short-term model. Yet, this topics appears to be again considerable correlated to one specific website (see Figure D.1.2).

[2] The topic *cryptomoney* appears in the medium-term model as well. However, as said in the main text, this topic is highly correlated with specific websites.

[3] In addition, one can observe a positive and significant coefficient for the trend variable in the newspaper and day fixed effects specification, suggesting that the likelihood of DoS attacks increases after there had been a higher interest in the website.

in the short- and medium-term. Figure D.4.6 displays that many of the topics that are positively related to DoS attacks in the medium-term level (*corruption*, *outages*, *sanctions*, *Colombia border*, *outages* and *child mortality*) are slightly negatively related in the short-term models in some specifications. The opposite is true for the medium-term level, where the topics *exiled opposition*, *petroleum*, *PDVSA* and *opposition candidate* are negatively related to DoS attacks. This finding supports the conclusion from above, highlighting that the motivation and timing to censor depends on the reporting of specific news. Furthermore, there are three topics *food policy*, *government-opposition dialog* and *music/entertainment* that are negatively related to the likelihood of DoS attacks in the short- and medium-term models. The first is mostly about government policies to distribute food, the second about the government-opposition dialog on the Dominican Republic, while the last topic is clearly non-political.

Fourth, I define my topic variables differently by aggregating the topic to its maximum value for the respective newspaper/day. The reason behind this is the assumption that not the salience of a topic is important but whether it appears at least once. Again, I before checked for collinear topics and newspapers and left highly correlated topics out. With regard to the short-term model, Figure D.4.8 still shows that the topics *petroleum*, *resignations*, *shortages*, and *exiled opposition* remain (borderline) significantly related to the likelihood of attacks. Additionally, reporting about *court sentences* appear to slightly increase the likelihood of DoS attacks in the short-term model. Concerning the medium-term model, Figure D.4.9 shows that *Maduro*, *national assembly*, *outages* and *healthcare shortages* stay significantly related, whereas the topics *Óscar Pérez*, *salary/prices*, *government-opposition dialog* and *election* become positively related to DoS attacks. While the *salary/prices* topic is related to the social and economic crisis category, it appears that the other topics indicate that the respective news outlet reports about unique political events, which increase the likelihood of attacks. Compared to the average proportion specification, the "effect" sizes for the maximum specification are much smaller, suggesting that the salience of topics matter more in influencing DoS attacks as in this case more citizens will read and notice the news.

Fifth, I define the dependent variable DoS attacks differently and consider (1) all 5XX error codes and (2) also refused connections (999 error codes). When I consider all 5XX error codes, the number of DoS attacks increases to 145 and even to 198 when I include the 999 error codes. This decreases potential estimation errors due to the higher number of events, yet increases potential measurement errors.

For the 5XX error code specification, the short-term results still show that the topics *PDVSA*, *Cuba*, *shortages healthcare*, *political prisoners* and *exiled opposition* remain/become (borderline) significantly related to the likelihood of attacks (see Figure D.4.10). This is also true for the topic *cryptomoney* that remains, however, highly correlated to one specific website. Furthermore, the topics *government ministers*, *salary/prices* and *education studies* become significantly related in this specification. The latter seems

again to be explained by a high correlation with one specific newspaper (see Figure D.1.2). For the medium-term models, news on *shortages healthcare*, *outages*, *shortages*, *Cuba*, *USA/Korea*, *government ministers*, *Maduro* and *corruption* are still significantly related to the likelihood of DoS attacks (see Figure D.4.11). In addition, the topics *airline opening/closing*, *political prisoners* and *earthquake/accidents* are now positively and significantly related to the likelihood of attacks. The analysis reveals that only the topic *exiled opposition* remains unique in the short-term models, suggesting that DoS attacks are primarily used as repressive censoring tool. However, contrary to the main operationalization of DoS attacks, which relies only on 503 error codes, it is also more likely that other internal server errors are wrongly considered as DoS attacks.

For the specification that additionally includes 999 error codes, the topics *shortages healthcare*, *Cuba*, *PDSVSA* as well as the mixed topic *mining/sport (mixed)* remain significantly related to the likelihood of DoS attacks in the short-term (see Figure D.4.12).[4] In addition, the topic *government ministers* is significantly related to a higher likelihood of DoS attacks for the specification including day and newspaper fixed effects. For the medium-term model, news on *government ministers* and *outages* stay significantly related to and the topics *airline opening/closing* and *mining/sport (mixed)* become now substantially related to the likelihood of DoS attacks (see Figure D.4.13). Again, only one topic (*PDVSA*) remains uniquely related to DoS attacks in the short-term model. Although this would rather speak for the use of DoS attacks as exclusive repressive tool, I cannot be sure whether the refused connection is due to the contacted server, my server or some machine in the middle. Hence, it is very likely that not only DoS attacks are captured.

Finally, I consider stronger attacks only and focus on DoS attacks were at least two subsequent measurement failed. Stronger attacks may indicate that the attacker used more resources and was more sincere in disabling the attacked websites. This may make it more likely that state-actors were behind these attacks. However, by adding this restriction, the number of DoS attacks decreases to 21 and the likelihood of estimation errors may increase. Overall, the results show a larger number of topics that are significantly related to a higher likelihood of DoS attacks.

For the short-term models these are similarly as in the main analysis the topics *resignations*, *PDVSA*, *shortages*, *Cuba* and *exiled opposition*.[5] Furthermore, the topics *International Organizations*, *political prisoners*, *election*, *mining/sport (mixed)*, *national assembly* and *Russia* show now significant marginal effects. The found relationship for the topic *Russia* may be likely explained by the fact that this topic positively correlates to the topic *USA/Korea* and *sanctions*. For the medium-term models the marginal effects for the topics *corruption*, *Maduro*, *church/job offer (mixed)*, *sanctions* and *Colombia border* show similar significant effects as in the main analysis. Besides, the topics

[4] As well as the topic *cryptomoney* were the above outlined concerns are still valid.

[5] In addition, the topic *cryptomoney* remains correlated as well.

protest/shortages, *Óscar Pérez*, *Cuba*, and *government ministers* show a significant correlation with the likelihood of DoS attacks.[6] This is also true for the topics *political prisoners*, *child mortality*, *migration crisis*, *International Organizations* and *resignations*, yet for these topics the effect sizes are smaller.

These results highlight that more topics are significantly related to a higher likelihood of DoS attacks in the medium-term. Besides, several of these topics overlaps in the short- and medium-term models. Nevertheless, some topics (*PDVSA*, *exiled opposition* and *resignations*) are still related to a higher likelihood of DoS attacks exclusively in the short-term. In conclusion, while these findings again support both censorship functions of DoS attacks, the repressive mechanism appears to be more pronounced.

[6]This is again observable for the topic *cryptomoney*, for which the above outlined concerns are still valid.

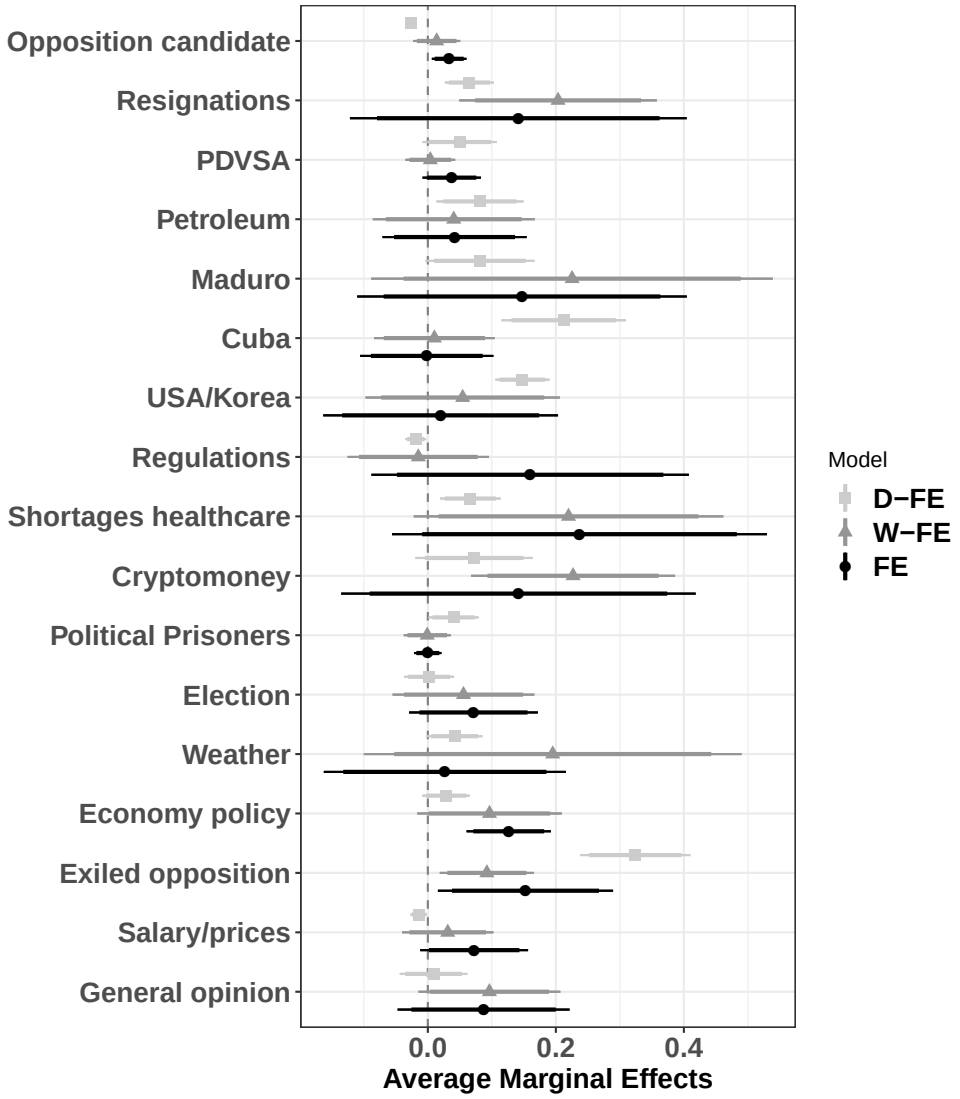

Figure D.4.1: Average Marginal Effects (AME) of significantly positively related topics (short-term models) on a news website's likelihood of receiving a DoS attack (average topic distribution incl. t-1). Simulations based on 1000 draws. Topics are not ordered according to broader categories.

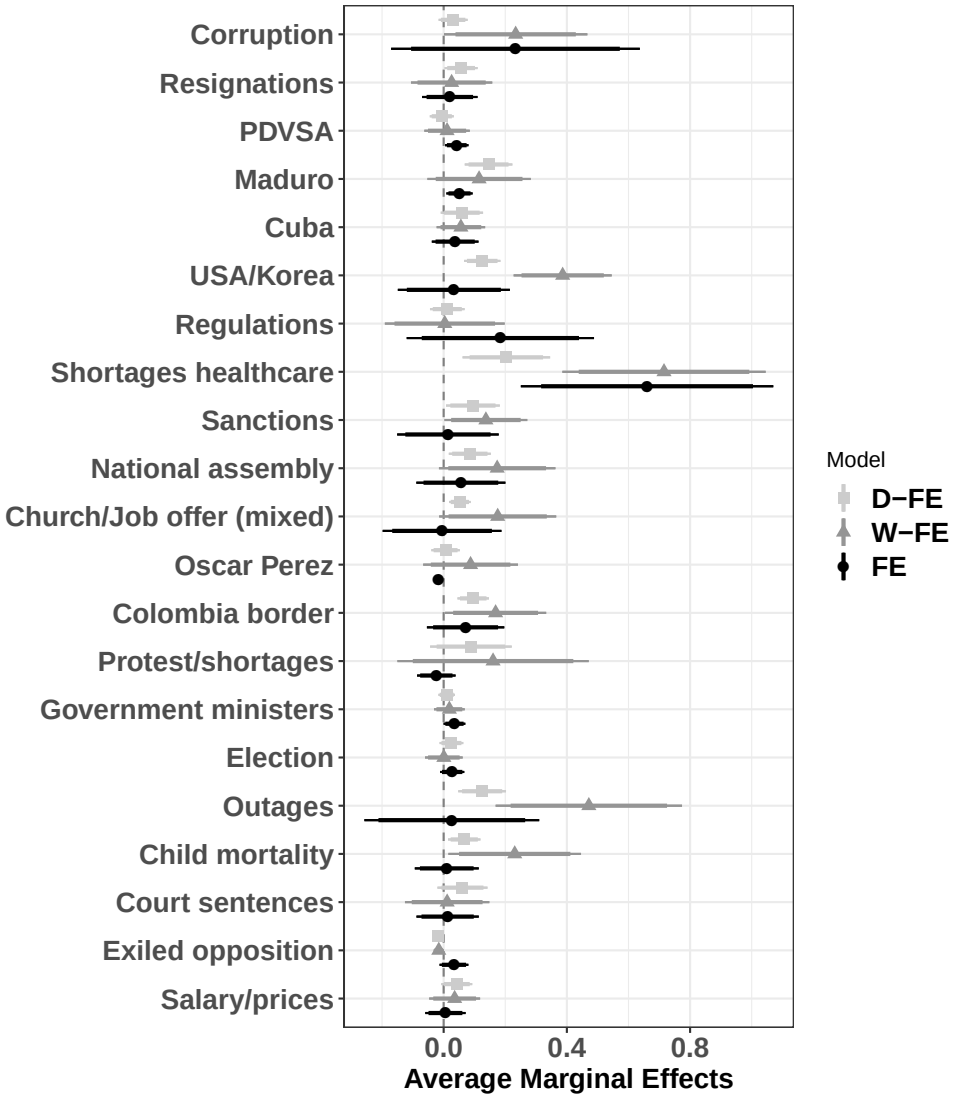

Figure D.4.2: AME of significantly positively related topics (medium-term models) on a news website's likelihood of receiving a DoS attack (average topic distribution from t-2 until t-7). Simulations based on 1000 draws.

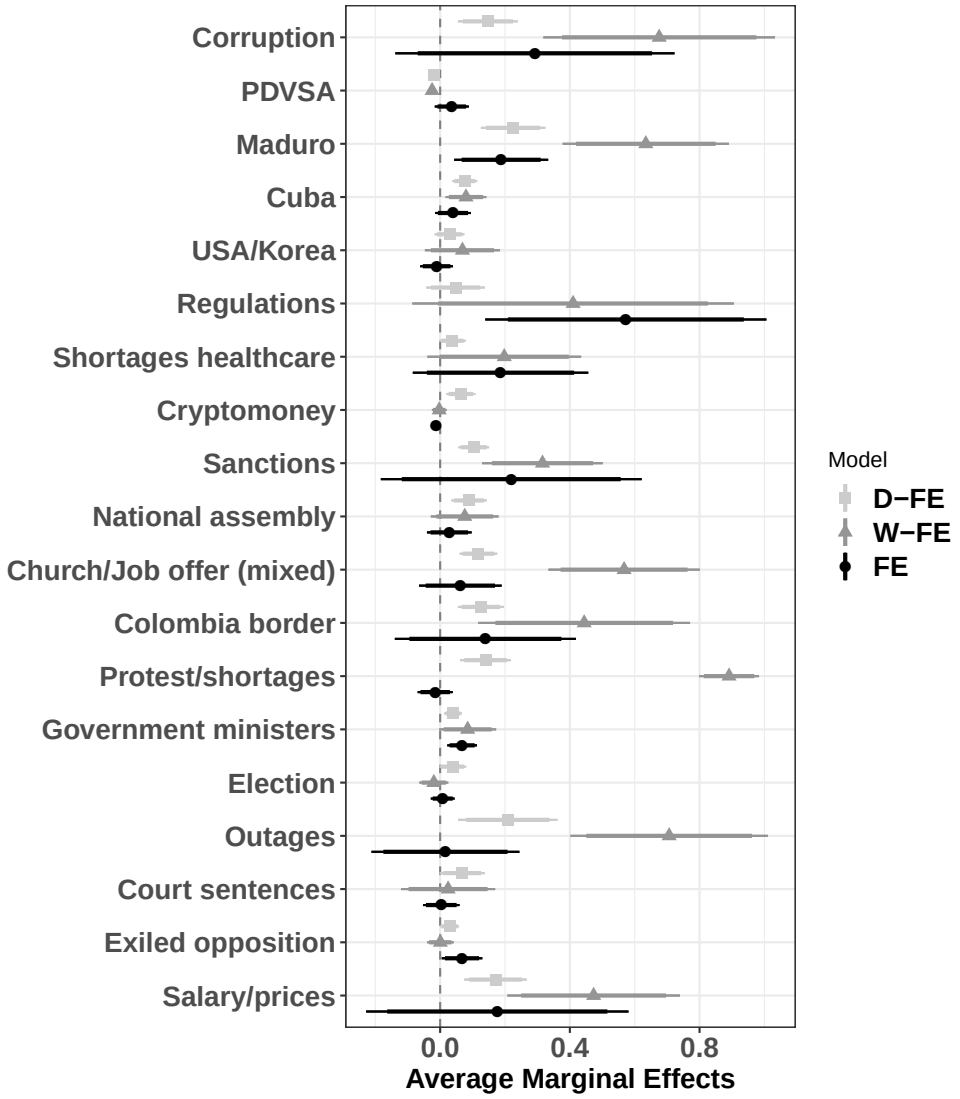

Figure D.4.3: AME of significantly positively related topics (medium-term models) on a news website's likelihood of receiving a DoS attack (average topic distribution up to 14 days before). Simulations based on 1000 draws.

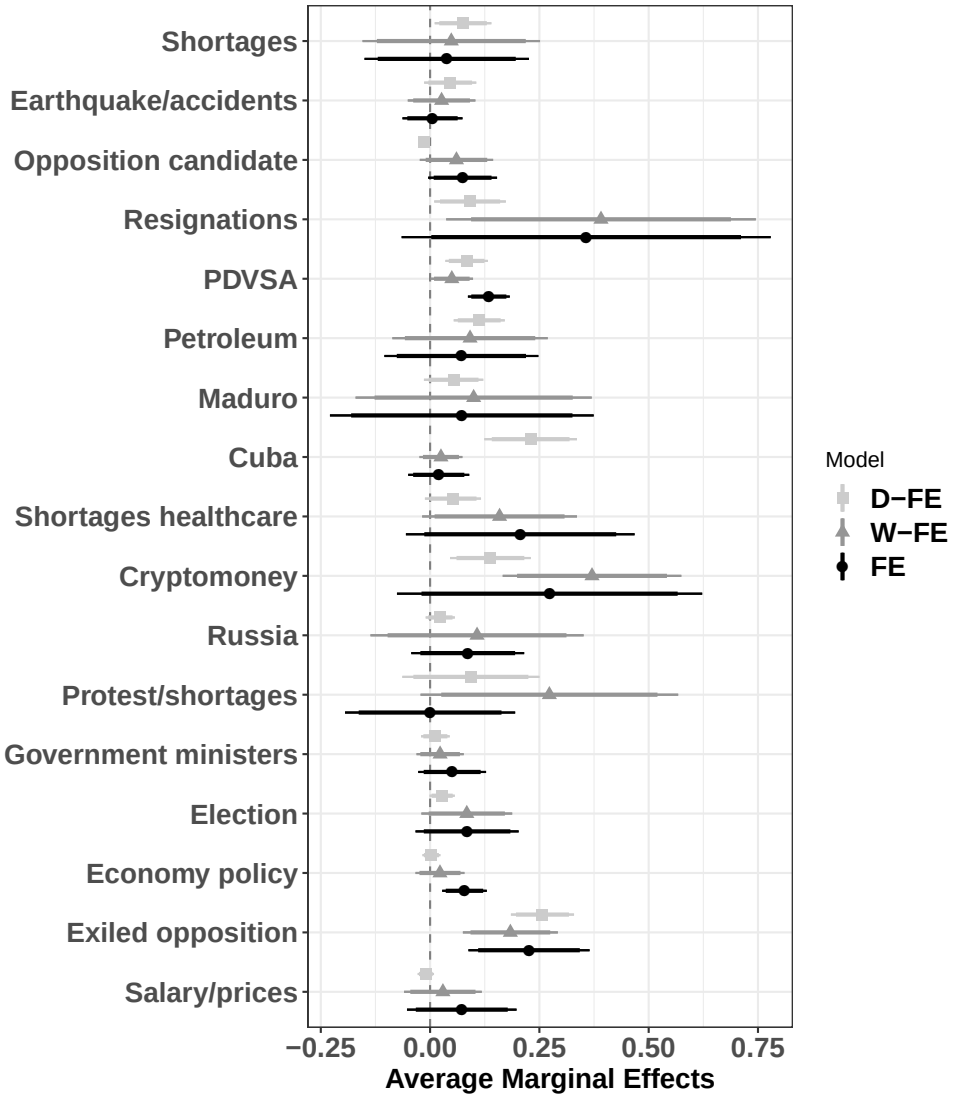

Figure D.4.4: AME of significantly positively related topics (short-term models) on a news website's likelihood of receiving a DoS attack (incl. Google trends). Simulations based on 1000 draws.

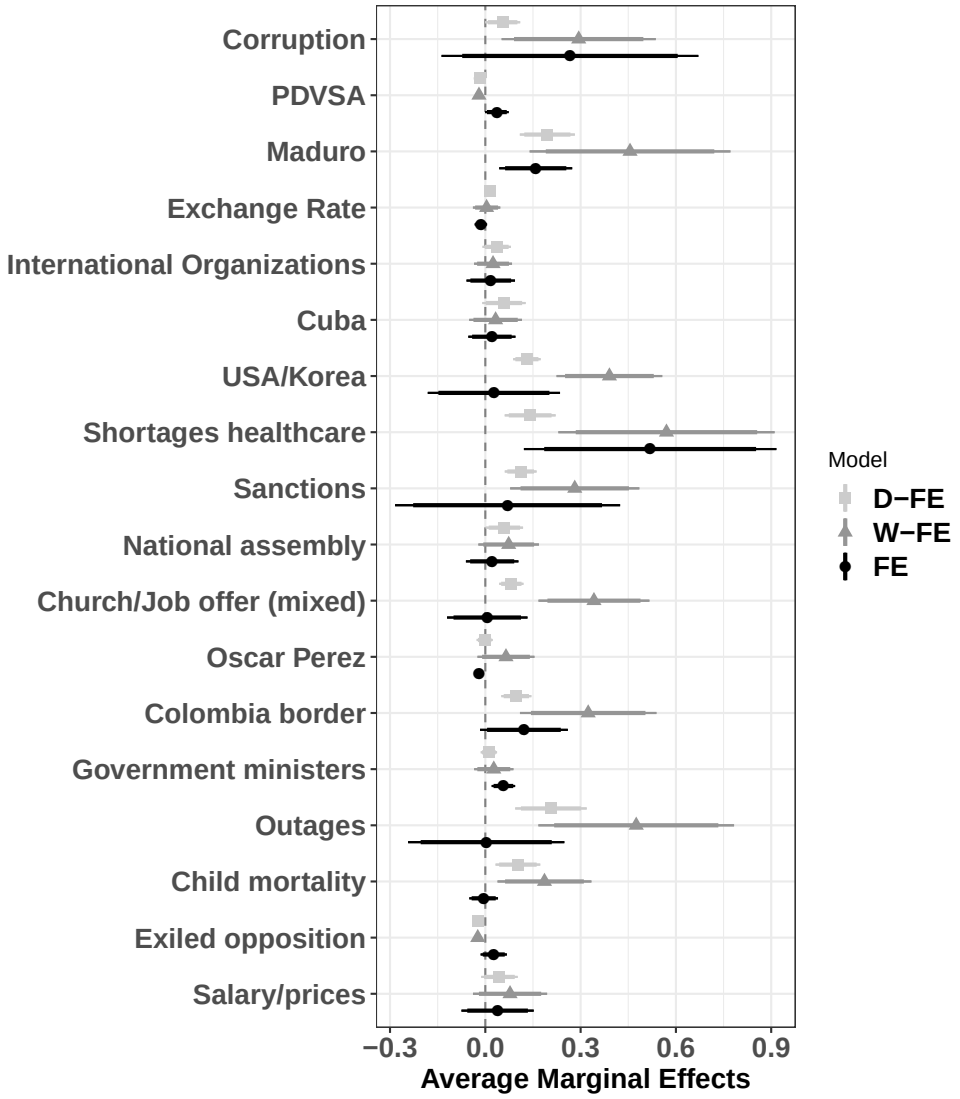

Figure D.4.5: AME of significantly positively related topics (medium-term models) on a news website's likelihood of receiving a DoS attack (incl. Google trends). Simulations based on 1000 draws.

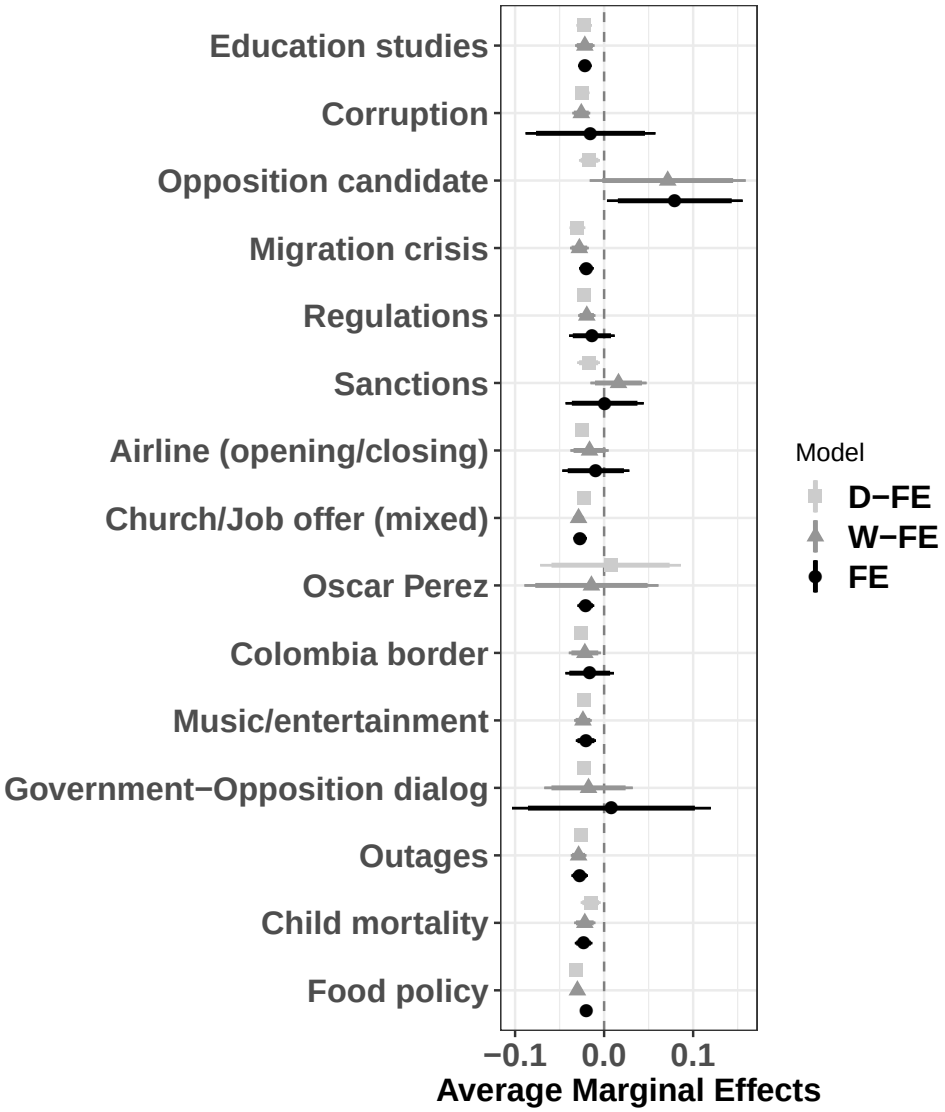

Figure D.4.6: AME of significantly negatively related topics (short-term models) on a news website's likelihood of receiving a DoS attack. Simulations based on 1000 draws.

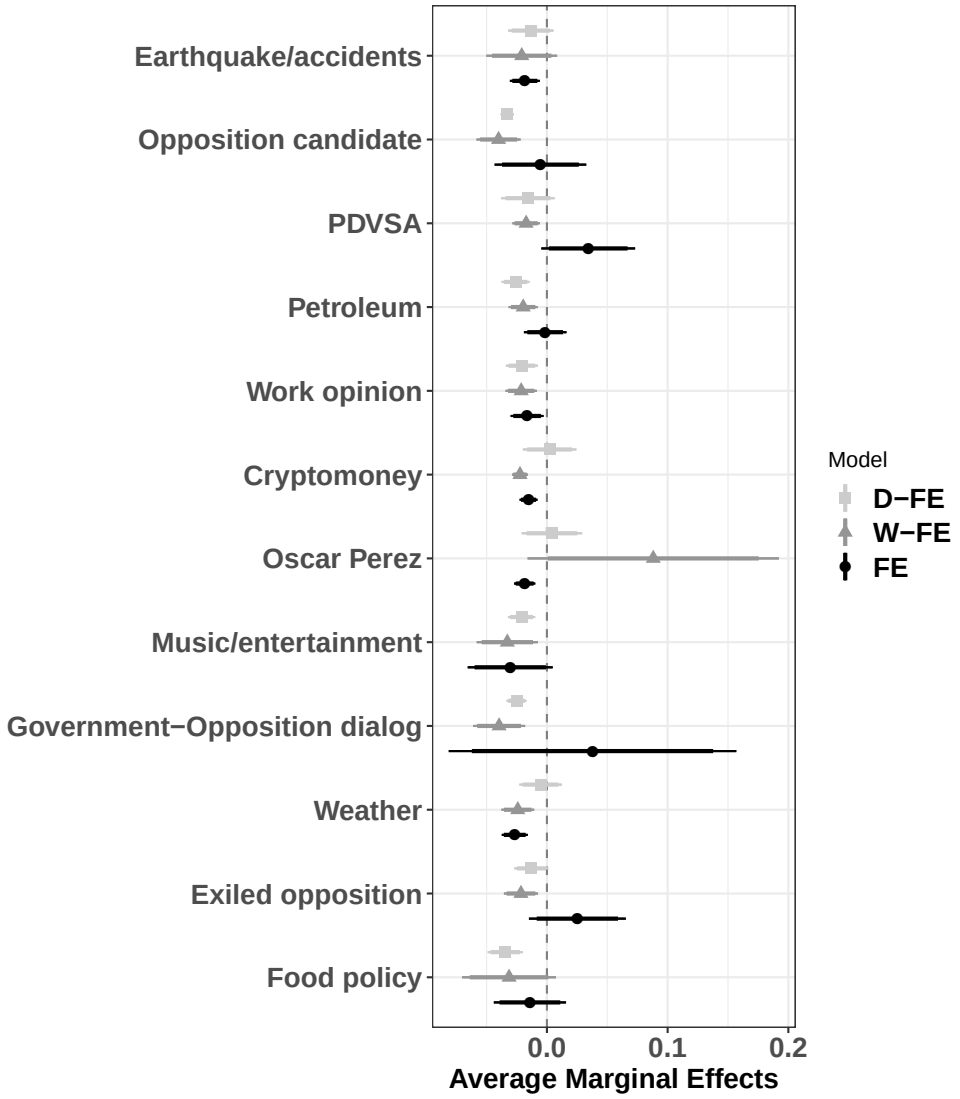

Figure D.4.7: AME of significantly negative related topics (medium-term models) on a news website's likelihood of receiving a DoS attack. Simulations based on 1000 draws.

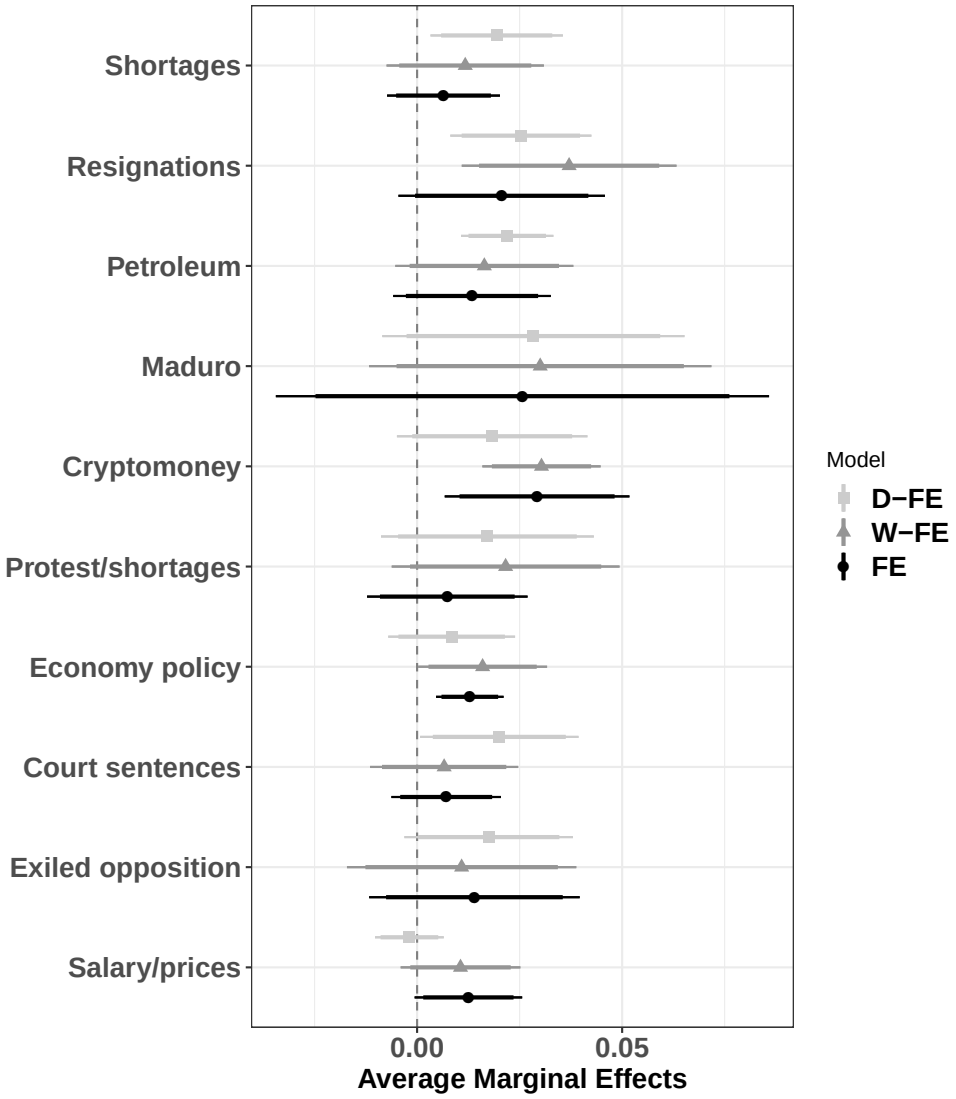

Figure D.4.8: AME of significantly positive related topics (short-term models) on a news website's likelihood of receiving a DoS attack (maximum proportion operationalization). Simulations based on 1000 draws.

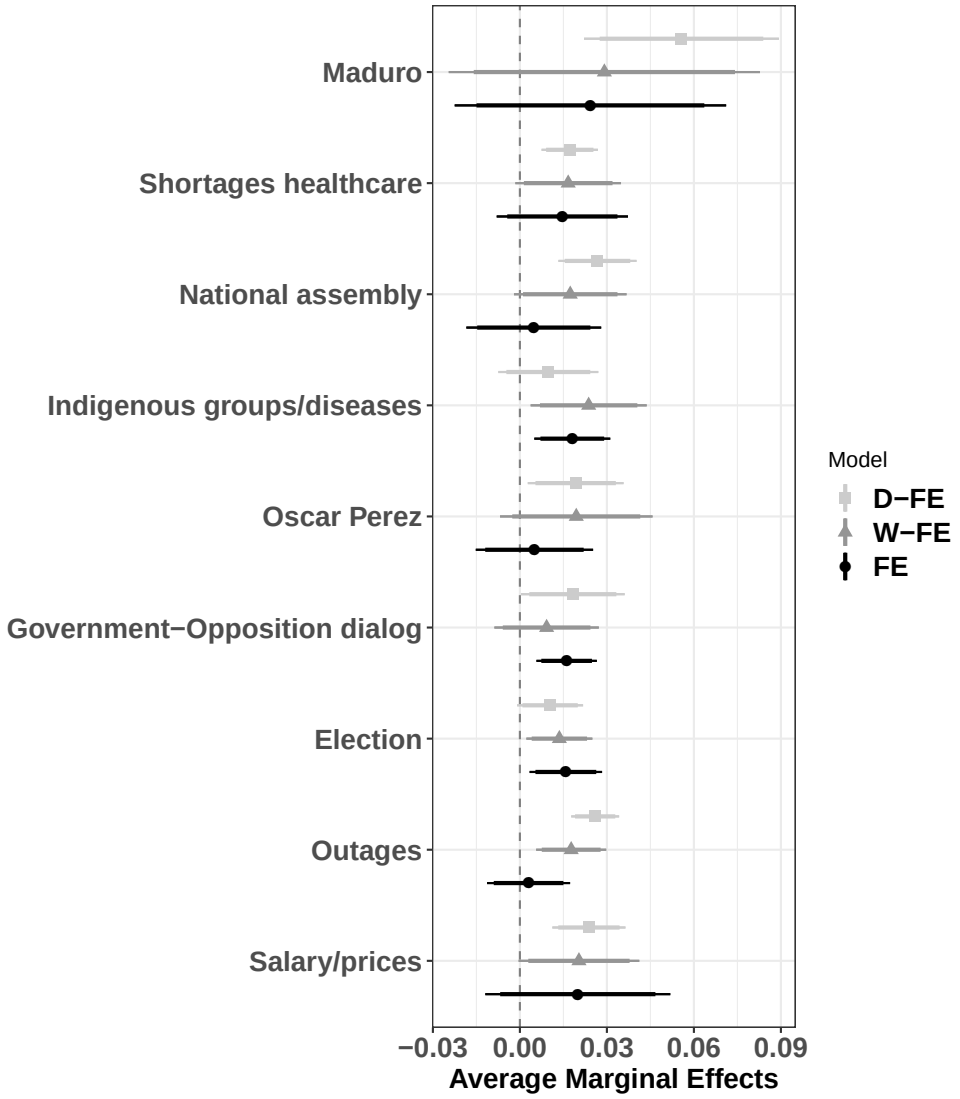

Figure D.4.9: AME of significantly positive related topics (medium-term models) on a news website's likelihood of receiving a DoS attack a specific day (maximum proportion operationalization). Simulations based on 1000 draws.

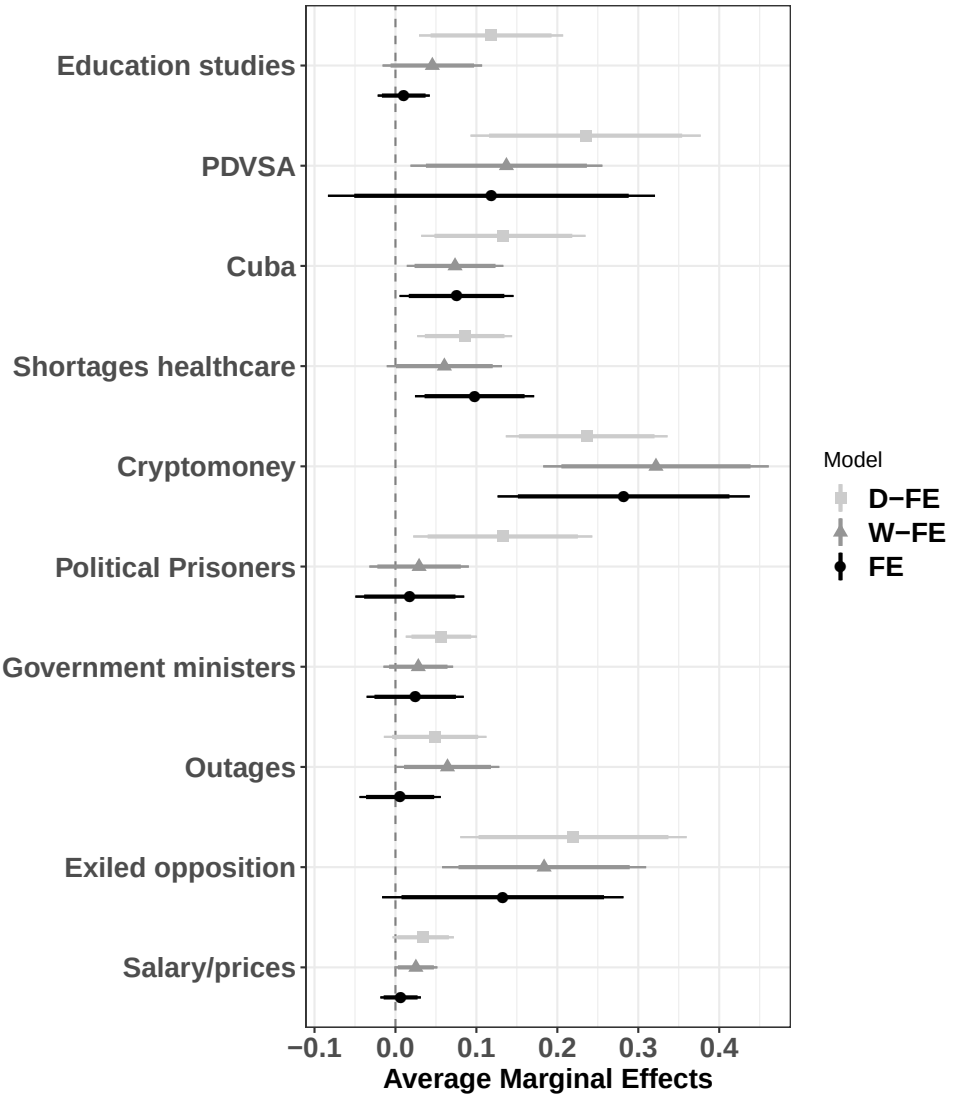

Figure D.4.10: AME of significantly positive related topics (short-term models) on a news website's likelihood of receiving a DoS attack (incl. all 5XX error codes). Simulations based on 1000 draws.

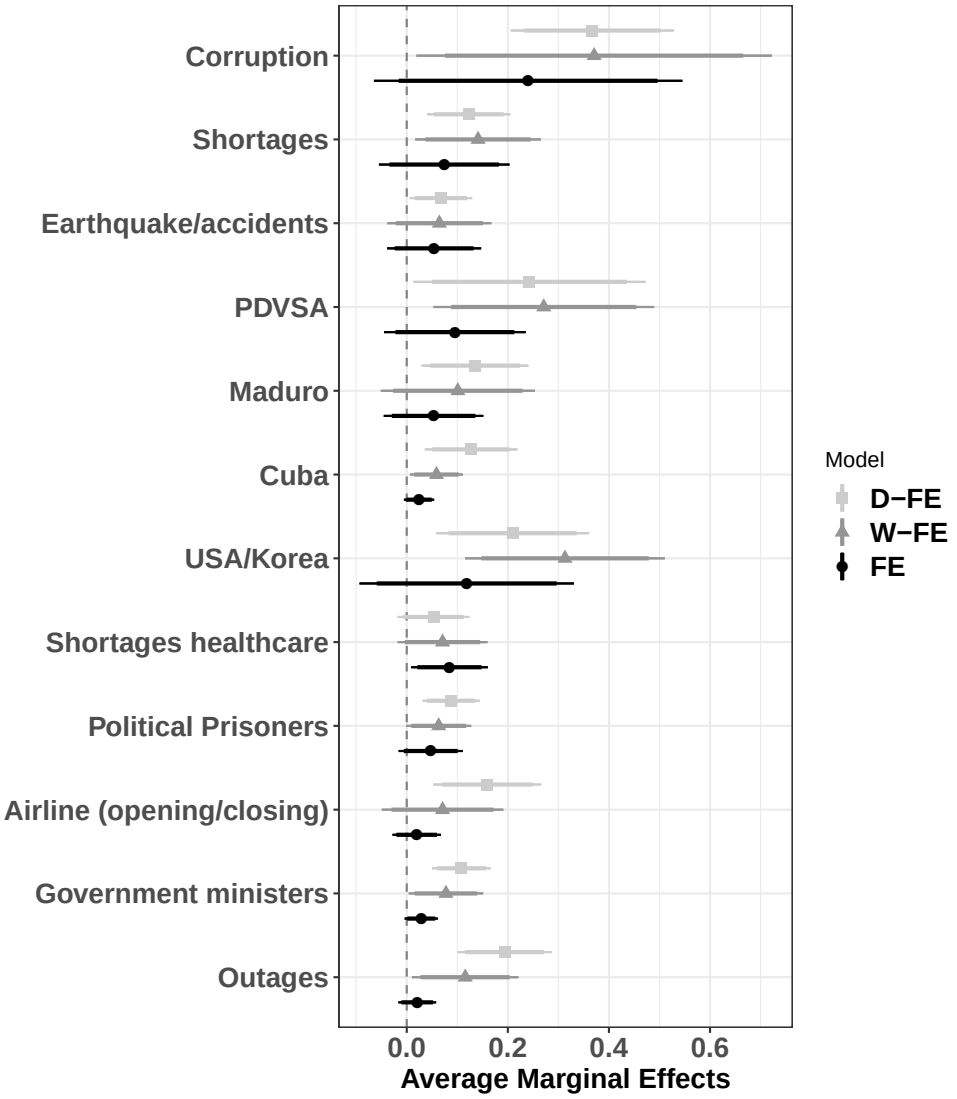

Figure D.4.11: AME of significantly positive related topics (medium-term models) on a news website's likelihood of receiving a DoS attack (incl. all 5XX error codes). Simulations based on 1000 draws.

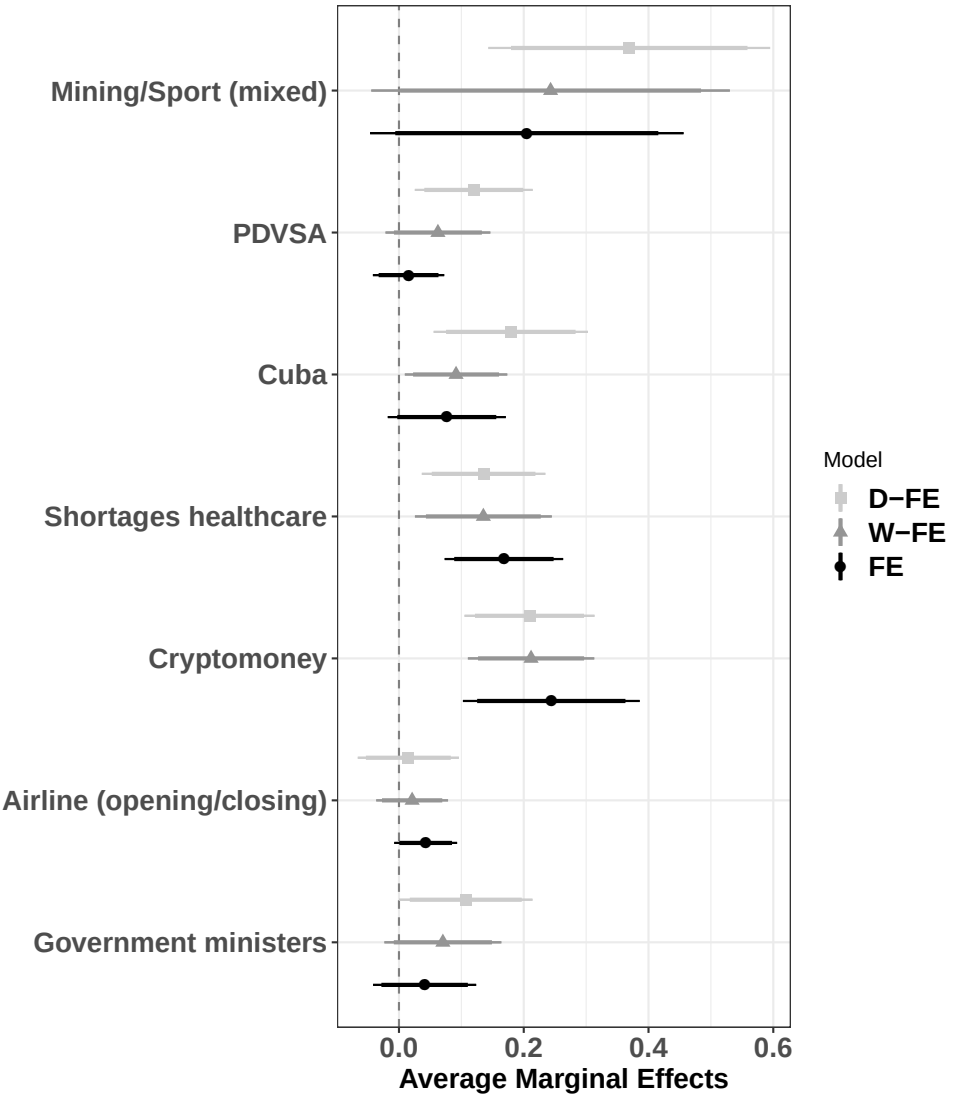

Figure D.4.12: AME of significantly positive related topics (short-term models) on a news website's likelihood of receiving a DoS attack (incl. all 999 error code). Simulations based on 1000 draws.

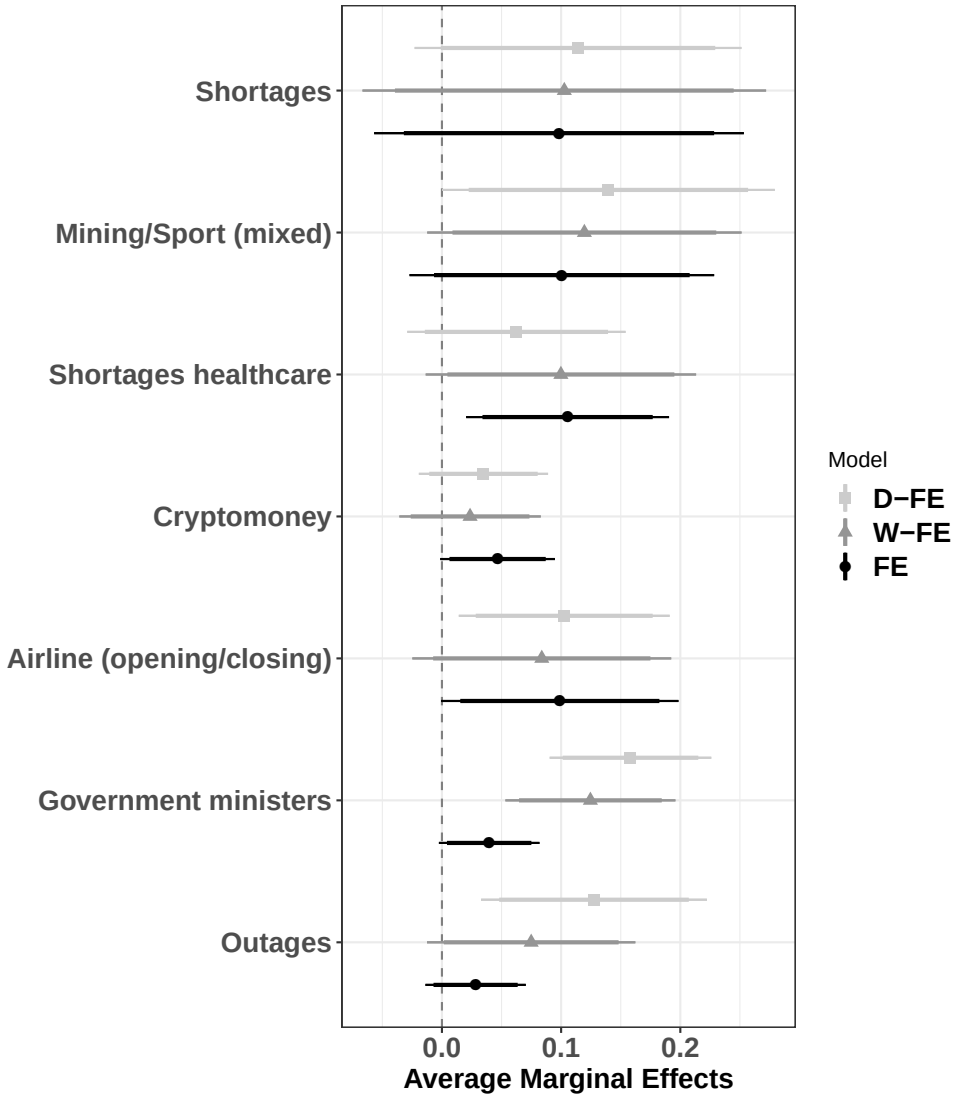

Figure D.4.13: AME of significantly positive related topics (medium-term models) on a news website's likelihood of receiving a DoS attack on a specific day (incl. all 999 error code). Simulations based on 1000 draws.

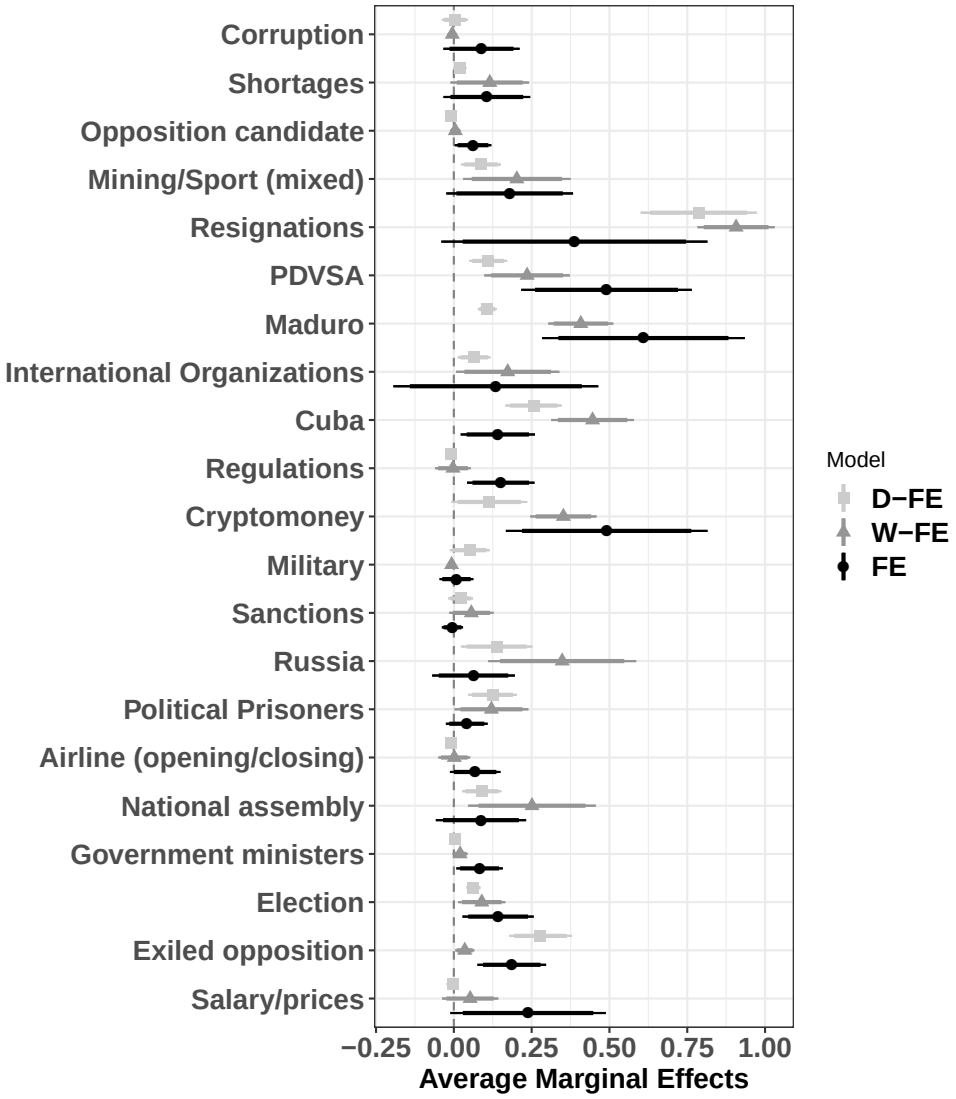

Figure D.4.14: AME of significantly positive related topics (short-term models) on a news website's likelihood of receiving a DoS attack (only strong attacks). Simulations based on 1000 draws.

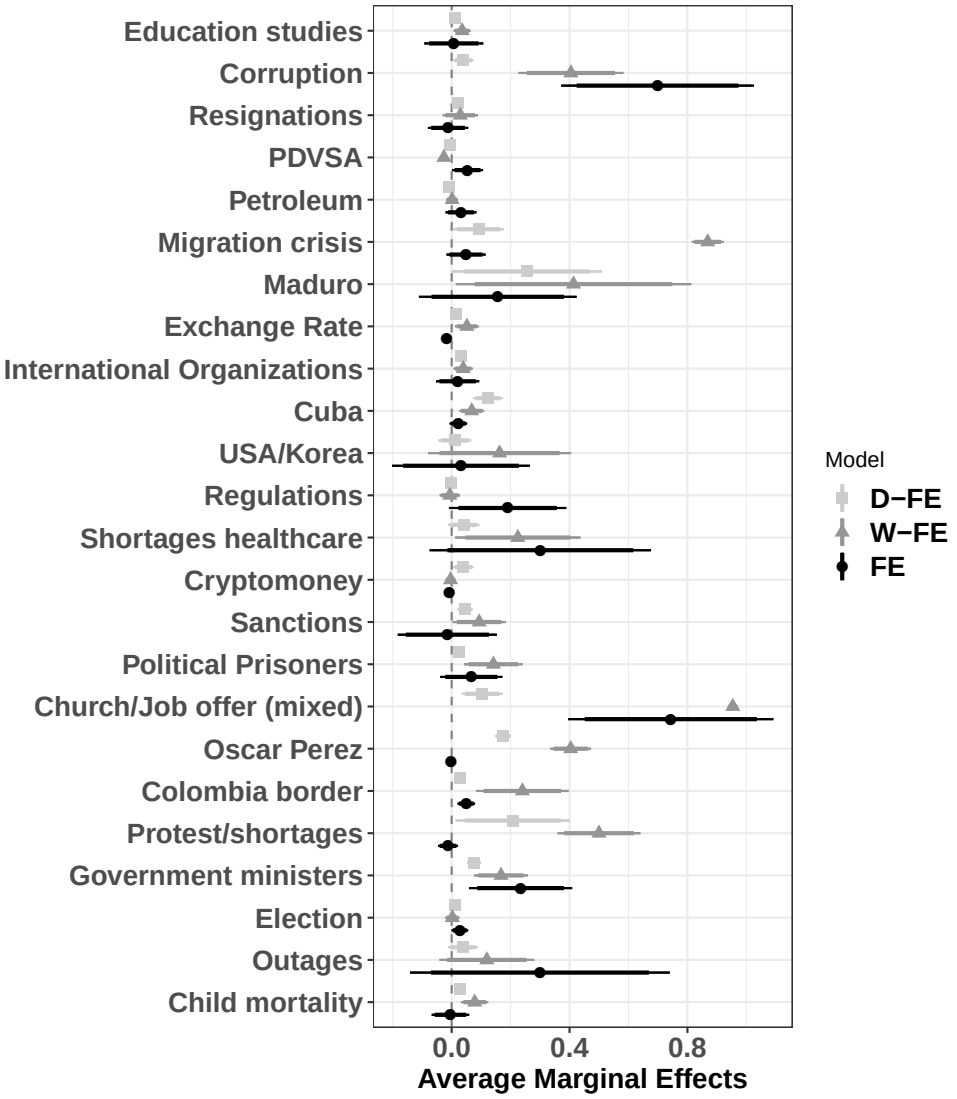

Figure D.4.15: AME of significantly positive related topics (medium-term models) on a news website's likelihood of receiving a DoS attack on a specific day (only strong attacks). Simulations based on 1000 draws.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.13	0.04	−0.38***	0.28***	0.28***	0.07	−0.39	−0.56	0.26	0.20	0.10	−0.61***	−0.07	−3.04***	−0.27	0.11	0.27	−0.10	−0.15	−0.23	0.08	−0.29**	0.12
	(0.20)	(0.14)	(0.10)	(0.04)	(0.05)	(0.12)	(0.21)	(0.29)	(0.14)	(0.16)	(0.16)	(0.09)	(0.25)	(0.68)	(0.32)	(0.12)	(0.14)	(0.13)	(0.17)	(0.19)	(0.11)	(0.09)	(0.07)
Number of headlines	0.05**	0.05**	0.05***	0.05**	0.05***	0.05***	0.06***	0.05**	0.05***	0.05**	0.05***	0.07***	0.05**	0.06***	0.05***	0.05**	0.05***	0.05***	0.05**	0.05**	0.05**	0.05**	0.05**
	(0.01)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.70***	2.71***	2.68***	2.69***	2.67***	2.71***	2.60***	2.62***	2.70***	2.67***	2.70***	2.50***	2.73***	2.53***	2.68***	2.68***	2.71***	2.69***	2.70***	2.67***	2.71***	2.70***	2.72***
	(0.58)	(0.60)	(0.59)	(0.59)	(0.56)	(0.60)	(0.54)	(0.59)	(0.59)	(0.61)	(0.59)	(0.55)	(0.60)	(0.53)	(0.60)	(0.57)	(0.60)	(0.59)	(0.60)	(0.61)	(0.59)	(0.60)	(0.60)
AIC	410.97	411.29	408.53	407.24	408.39	411.35	407.79	407.01	410.05	410.07	411.16	401.80	411.04	400.34	409.69	410.55	409.56	410.70	410.40	410.11	411.16	409.59	411.10
BIC	435.66	435.98	433.23	431.94	433.09	436.04	432.49	431.71	434.74	434.77	435.86	426.49	435.74	425.03	434.38	435.25	434.25	435.40	435.10	434.81	435.86	434.28	435.80
Log Likelihood	-201.48	-201.64	-200.27	-199.62	-200.19	-201.67	-199.90	-199.51	-201.02	-201.04	-201.58	-196.90	-201.52	-196.17	-200.84	-201.28	-200.78	-201.35	-201.20	-201.06	-201.58	-200.79	-201.55
Deviance	402.97	403.29	400.53	399.24	400.39	403.35	399.79	399.01	402.05	402.07	403.16	393.80	403.04	392.34	401.69	402.55	401.56	402.70	402.40	402.11	403.16	401.59	403.10
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.33***	0.19	−0.13	0.04	−0.09	−0.06	0.26**	0.05	−0.06	−0.01	0.15	−0.44	−0.24	0.41***	0.26**	0.29***	−0.56	0.06	0.23	−0.14	−0.16	−0.02	−0.59***
	(0.08)	(0.17)	(0.20)	(0.18)	(0.21)	(0.11)	(0.11)	(0.12)	(0.10)	(0.19)	(0.21)	(0.25)	(0.14)	(0.10)	(0.10)	(0.06)	(0.44)	(0.11)	(0.14)	(0.20)	(0.11)	(0.17)	(0.36)
Number of headlines	0.05***	0.05***	0.05***	0.05**	0.05***	0.05**	0.06***	0.05***	0.05**	0.05***	0.05**	0.05**	0.05***	0.06***	0.05***	0.05***	0.07***	0.05**	0.05***	0.05**	0.05**	0.05***	0.06***
	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)
DoS attack (t-1)	2.55***	2.68***	2.68***	2.70***	2.69***	2.71***	2.69***	2.71***	2.71***	2.71***	2.71***	2.67***	2.70***	2.58***	2.65***	2.65***	2.58***	2.71***	2.70***	2.71***	2.70***	2.71***	2.54***
	(0.56)	(0.58)	(0.58)	(0.59)	(0.60)	(0.59)	(0.56)	(0.61)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)	(0.58)	(0.60)	(0.60)	(0.51)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)	(0.54)
AIC	405.44	410.26	410.50	411.33	410.87	410.93	406.69	411.41	411.10	411.23	410.67	408.59	409.74	405.06	409.32	408.01	405.24	411.23	410.16	410.64	410.28	410.98	402.10
BIC	430.14	434.95	435.19	436.02	435.57	435.63	431.38	436.11	435.79	435.93	435.37	433.29	434.40	429.76	434.02	432.70	429.94	435.90	434.86	435.34	434.97	435.68	426.80
Log Likelihood	-198.72	-201.13	-201.25	-201.66	-201.44	-201.47	-199.34	-201.71	-201.55	-201.62	-201.34	-200.30	-200.85	-198.53	-200.66	-200.00	-198.62	-201.60	-201.08	-201.32	-201.14	-201.49	-197.05
Deviance	397.44	402.26	402.50	403.33	402.87	402.93	398.69	403.41	403.10	403.23	402.67	400.59	401.71	397.06	401.32	400.01	397.24	403.21	402.16	402.64	402.28	402.98	394.10
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.1: Penalized logistic regression results - short-term (t & t-1) models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.33*	0.24**	−0.31***	0.24***	−0.05	0.32***	−0.44***	−0.75***	0.15	0.31*	0.14	−0.52***	0.15	−0.38	0.11	−0.43***	−0.41*	−0.17	−0.35**	−0.00	0.10
	(0.13)	(0.08)	(0.09)	(0.05)	(0.09)	(0.04)	(0.17)	(0.17)	(0.23)	(0.12)	(0.15)	(0.15)	(0.13)	(0.25)	(0.16)	(0.09)	(0.17)	(0.18)	(0.12)	(0.06)	(0.07)
DoS attack (t-1)	2.07***	2.04***	2.06***	2.04***	2.05***	2.04***	2.00***	1.94***	2.07***	2.04**	2.05***	2.04***	2.03***	2.02***	2.07***	2.05***	1.98***	2.05***	2.05***	2.06***	2.04***
	(0.36)	(0.36)	(0.35)	(0.37)	(0.36)	(0.36)	(0.34)	(0.39)	(0.36)	(0.35)	(0.36)	(0.36)	(0.35)	(0.37)	(0.37)	(0.36)	(0.36)	(0.36)	(0.37)	(0.36)	(0.36)
AIC	411.96	411.48	410.77	409.86	411.91	411.54	409.61	407.08	412.47	409.79	412.06	410.49	411.87	410.78	412.13	409.54	410.40	411.56	410.47	412.07	411.79
BIC	542.04	541.56	540.86	539.95	542.00	541.62	539.70	537.16	542.56	539.87	542.14	540.58	541.96	540.86	542.21	539.63	540.49	541.64	540.56	542.16	541.88
Log Likelihood	-184.98	-184.74	-184.39	-183.93	-184.96	-184.77	-183.81	-182.54	-185.24	-183.89	-185.03	-184.25	-184.94	-184.39	-185.06	-183.77	-184.20	-184.78	-184.24	-185.04	-184.90
Deviance	369.96	369.48	368.77	367.86	369.91	369.54	367.61	365.08	370.47	367.79	370.06	368.49	369.87	368.78	370.13	367.54	368.40	369.56	368.47	370.07	369.79
Num. obs.	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.03	−0.05	0.38*	0.36**	0.23**	0.12	−0.01	−0.12	−0.18	0.52*	−0.03	−0.32***	0.22	0.15**	0.20*	0.07	0.23***	0.06	0.06	0.06	−0.75***
	(0.19)	(0.16)	(0.18)	(0.11)	(0.09)	(0.24)	(0.11)	(0.14)	(0.11)	(0.23)	(0.15)	(0.08)	(0.16)	(0.06)	(0.09)	(0.24)	(0.06)	(0.17)	(0.18)	(0.15)	(0.17)
DoS attack (t-1)	2.06***	2.05***	2.01***	2.06***	2.04***	2.08***	2.06***	2.05***	2.05***	2.09***	2.05***	2.09***	2.03**	2.04***	2.02***	2.05***	2.04***	2.05***	2.05***	2.06***	2.02***
	(0.36)	(0.36)	(0.32)	(0.36)	(0.36)	(0.38)	(0.36)	(0.35)	(0.36)	(0.32)	(0.36)	(0.36)	(0.36)	(0.36)	(0.39)	(0.36)	(0.36)	(0.36)	(0.36)	(0.36)	(0.34)
AIC	412.12	411.98	410.96	410.82	413.04	411.89	412.13	411.59	411.52	407.81	412.34	410.55	411.21	411.89	411.80	412.22	411.49	412.19	412.26	412.24	408.44
BIC	542.20	542.07	541.05	540.90	543.12	541.97	542.21	541.67	541.61	537.89	542.42	540.63	541.30	541.97	541.88	542.30	541.57	542.27	542.35	542.33	538.53
Log Likelihood	-185.06	-184.99	-184.48	-184.41	-185.52	-184.94	-185.06	-184.79	-184.76	-182.90	-185.17	-184.27	-184.61	-184.94	-184.90	-185.11	-184.74	-185.09	-185.13	-185.12	-183.22
Deviance	370.12	369.98	368.96	368.82	371.04	369.89	370.13	369.59	369.52	365.81	370.34	368.55	369.21	369.89	369.80	370.22	369.49	370.19	370.26	370.24	366.44
Num. obs.	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621

Table D.4.2: Penalized logistic regression results - short-term (t & t-1) models (newspaper fixed effects). Note: Newspaper fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.33**	0.13	−0.67***	0.18***	−0.12	0.27**	−0.19	−0.53***	0.46*	0.25	−0.19	−0.51**	0.01	−0.00	0.11	−0.14	−0.09	−0.06	−0.43***	−0.00	0.09
	(0.11)	(0.09)	(0.13)	(0.04)	(0.16)	(0.09)	(0.15)	(0.13)	(0.19)	(0.15)	(0.15)	(0.18)	(0.13)	(0.14)	(0.13)	(0.09)	(0.09)	(0.10)	(0.11)	(0.08)	(0.10)
DoS attack (t-1)	1.54***	1.53***	1.52***	1.54***	1.53***	1.52***	1.52***	1.47***	1.56***	1.54***	1.52***	1.51***	1.53***	1.53***	1.55***	1.54***	1.52***	1.54***	1.54***	1.53***	1.52***
	(0.32)	(0.32)	(0.30)	(0.32)	(0.32)	(0.32)	(0.32)	(0.32)	(0.32)	(0.32)	(0.32)	(0.32)	(0.33)	(0.33)	(0.33)	(0.32)	(0.33)	(0.32)	(0.33)	(0.32)	(0.32)
AIC	436.86	437.11	433.48	436.19	436.69	436.84	436.79	435.05	437.26	436.19	436.55	435.46	437.24	437.36	437.24	437.03	437.23	437.11	435.03	437.15	436.89
BIC	709.41	709.67	706.04	708.75	709.24	709.40	709.34	707.60	709.82	708.75	709.11	708.02	709.80	709.92	709.79	709.59	709.79	709.67	707.59	709.71	709.45
Log Likelihood	-174.43	-174.55	-172.74	-174.10	-174.34	-174.42	-174.39	-173.52	-174.63	-174.10	-174.28	-173.73	-174.62	-174.68	-174.62	-174.51	-174.61	-174.56	-173.51	-174.58	-174.44
Deviance	348.86	349.11	345.48	348.19	348.69	348.84	348.79	347.05	349.26	348.19	348.55	347.46	349.24	349.36	349.24	349.03	349.23	349.11	347.03	349.15	348.89
Num. obs.	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.16	−0.04	0.47***	0.35**	−0.12	0.23	0.03	−0.09	−0.11	0.64*	0.04	−0.45***	0.20	0.02	0.24***	0.13	0.11	0.16	0.07	−0.23	−0.53***
	(0.13)	(0.18)	(0.09)	(0.11)	(0.18)	(0.17)	(0.08)	(0.12)	(0.09)	(0.25)	(0.10)	(0.10)	(0.18)	(0.08)	(0.05)	(0.19)	(0.11)	(0.12)	(0.18)	(0.12)	(0.11)
DoS attack (t-1)	1.52***	1.53***	1.47***	1.55***	1.54***	1.55***	1.53***	1.53***	1.53***	1.56**	1.54***	1.58***	1.53***	1.53***	1.50***	1.53***	1.53***	1.53***	1.53***	1.50***	1.53***
	(0.33)	(0.32)	(0.29)	(0.32)	(0.32)	(0.33)	(0.32)	(0.32)	(0.33)	(0.27)	(0.32)	(0.32)	(0.33)	(0.33)	(0.34)	(0.33)	(0.33)	(0.33)	(0.32)	(0.34)	(0.31)
AIC	437.09	437.11	435.80	435.81	437.24	436.45	437.37	436.98	437.10	432.68	437.50	434.91	436.49	437.25	436.48	437.36	437.28	437.05	437.38	436.34	435.67
BIC	709.65	709.67	708.36	708.37	709.80	709.01	709.93	709.54	709.66	705.24	710.06	707.47	709.05	709.81	709.04	709.91	709.84	709.60	709.94	708.90	708.23
Log Likelihood	-174.55	-174.56	-173.90	-173.90	-174.62	-174.23	-174.69	-174.49	-174.55	-172.34	-174.75	-173.45	-174.25	-174.62	-174.24	-174.68	-174.64	-174.52	-174.69	-174.17	-173.84
Deviance	349.09	349.11	347.80	347.81	349.24	348.45	349.37	348.98	349.10	344.68	349.50	346.91	348.49	349.25	348.48	349.36	349.28	349.05	349.38	348.34	347.67
Num. obs.	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621

Table D.4.3: Penalized logistic regression results - short-term (t & t-1) models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.07	−0.15	−1.02***	0.63***	0.02	0.16*	0.11	−0.52***	0.25*	0.02	−0.21*	−0.37**	0.02	−0.36**	−0.14	−0.26*	0.03	−0.09	−0.62***	0.16**	0.08
	(0.17)	(0.09)	(0.12)	(0.05)	(0.10)	(0.08)	(0.06)	(0.06)	(0.10)	(0.16)	(0.09)	(0.13)	(0.13)	(0.12)	(0.09)	(0.11)	(0.09)	(0.19)	(0.07)	(0.06)	(0.05)
DoS attack (t-1)	2.94***	2.95***	2.99***	3.12***	2.95***	2.96***	2.96***	2.91***	2.96***	2.94***	2.93***	2.92***	2.93**	2.95***	2.92***	2.95***	2.95***	2.95***	2.90***	2.99***	2.95***
	(0.38)	(0.39)	(0.31)	(0.41)	(0.38)	(0.38)	(0.39)	(0.37)	(0.38)	(0.39)	(0.39)	(0.37)	(0.41)	(0.38)	(0.40)	(0.38)	(0.39)	(0.39)	(0.39)	(0.38)	(0.38)
AIC	353.94	353.42	345.80	348.08	353.65	353.86	353.88	352.27	353.91	353.79	353.43	352.25	353.77	352.73	353.37	353.15	354.01	353.56	350.91	353.51	353.50
BIC	750.39	749.87	742.25	744.53	750.09	750.31	750.33	748.72	750.36	750.23	749.88	748.70	750.22	749.18	749.82	749.60	750.46	750.01	747.36	749.96	749.95
Log Likelihood	-112.97	-112.71	-108.90	-110.04	-112.82	-112.93	-112.94	-112.13	-112.96	-112.89	-112.71	-112.13	-112.89	-112.37	-112.69	-112.58	-113.01	-112.78	-111.45	-112.75	-112.75
Deviance	225.94	225.42	217.80	220.08	225.65	225.86	225.88	224.27	225.91	225.79	225.43	224.25	225.77	224.73	225.37	225.15	226.01	225.56	222.91	225.51	225.50
Num. obs.	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.05	0.12	0.35*	0.24***	−0.25	0.58***	0.38***	−0.02	0.03	0.48*	−0.03	−0.47**	0.42**	0.22*	0.17***	0.26	−0.44***	0.22	0.13	−0.03	−0.38***
	(0.06)	(0.14)	(0.17)	(0.06)	(0.14)	(0.07)	(0.07)	(0.11)	(0.07)	(0.20)	(0.08)	(0.17)	(0.14)	(0.10)	(0.04)	(0.15)	(0.07)	(0.14)	(0.12)	(0.12)	(0.10)
DoS attack (t-1)	2.93***	2.94***	2.85***	2.90***	2.93***	3.01***	3.04***	2.94***	2.95***	2.82***	2.95***	3.00***	2.91***	2.96***	2.93***	2.93**	2.98***	2.93**	2.94***	2.93***	2.90***
	(0.38)	(0.39)	(0.38)	(0.38)	(0.40)	(0.37)	(0.39)	(0.38)	(0.39)	(0.35)	(0.39)	(0.36)	(0.39)	(0.38)	(0.41)	(0.39)	(0.37)	(0.40)	(0.38)	(0.40)	(0.37)
AIC	353.82	353.94	353.15	352.93	353.14	347.54	351.61	353.55	353.92	351.30	354.03	351.90	349.97	353.34	353.56	353.41	351.74	353.26	353.77	353.83	352.86
BIC	750.27	750.39	749.60	749.38	749.58	743.99	748.06	749.99	750.37	747.74	750.48	748.35	746.42	749.78	750.01	749.86	748.19	749.71	750.21	750.27	749.31
Log Likelihood	-112.91	-112.97	-112.58	-112.47	-112.57	-109.77	-111.81	-112.77	-112.96	-111.65	-113.02	-111.95	-110.98	-112.67	-112.78	-112.70	-111.87	-112.63	-112.88	-112.91	-112.43
Deviance	225.82	225.94	225.15	224.93	225.14	219.54	223.61	225.55	225.92	223.30	226.03	223.90	221.97	225.34	225.56	225.41	223.74	225.26	225.77	225.83	224.86
Num. obs.	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621	3621

Table D.4.4: Penalized logistic regression results - short-term (t & t-1) models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	−0.01	−0.15	−0.47	0.29***	0.30***	−0.20	−0.13	−0.08	0.21	0.10	0.09	−0.64***	−0.03	−2.37***	−0.31	0.05	0.36***	−0.00	−0.16	−0.01	0.28*	−0.10	0.22
	(0.31)	(0.28)	(0.19)	(0.08)	(0.08)	(0.25)	(0.21)	(0.21)	(0.17)	(0.13)	(0.19)	(0.14)	(0.25)	(0.65)	(0.33)	(0.12)	(0.10)	(0.13)	(0.14)	(0.28)	(0.14)	(0.19)	(0.15)
Number of headlines	0.05**	0.05***	0.06***	0.06***	0.06***	0.05***	0.06***	0.05***	0.06***	0.05***	0.05***	0.07***	0.05***	0.06***	0.05***	0.05**	0.06***	0.05***	0.05***	0.05***	0.06***	0.05***	0.05***
	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.02)	(0.02)	(0.01)	(0.02)
DoS attack (t-1)	2.72***	2.71***	2.67***	2.67***	2.65***	2.71***	2.68***	2.72***	2.70***	2.71***	2.70***	2.45***	2.72***	2.57***	2.66***	2.70***	2.63***	2.71***	2.70***	2.72***	2.71***	2.70***	2.70***
	(0.60)	(0.60)	(0.58)	(0.63)	(0.55)	(0.59)	(0.60)	(0.60)	(0.60)	(0.61)	(0.59)	(0.50)	(0.60)	(0.57)	(0.60)	(0.58)	(0.59)	(0.60)	(0.61)	(0.60)	(0.60)	(0.61)	(0.60)
AIC	399.49	398.86	396.64	396.04	393.60	398.38	398.87	399.29	398.95	399.33	399.43	389.24	399.46	391.54	397.62	399.36	395.76	399.50	398.58	399.49	397.46	399.08	398.11
BIC	424.16	423.53	421.31	420.71	418.27	423.05	423.54	423.96	423.62	424.00	424.10	413.91	424.13	416.21	422.29	424.03	420.43	424.17	423.25	424.16	422.13	423.74	422.78
Log Likelihood	-195.75	-195.43	-194.32	-194.02	-192.80	-195.19	-195.43	-195.65	-195.48	-195.66	-195.71	-190.62	-195.73	-191.77	-194.81	-195.68	-193.88	-195.75	-195.29	-195.75	-194.73	-195.54	-195.05
Deviance	391.49	390.86	388.64	388.04	385.60	390.38	390.87	391.29	390.95	391.33	391.43	381.24	391.46	383.54	389.62	391.36	387.76	391.50	390.58	391.49	389.46	391.08	390.11
Num. obs.	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.32*	0.29*	−0.16	0.18	−0.11	0.01	0.51***	0.10	0.29*	0.03	0.01	−1.10**	−0.20	0.32	0.26*	0.30***	−0.80*	−0.11	0.22	−0.28	−0.14	0.10	−0.92***
	(0.13)	(0.12)	(0.16)	(0.13)	(0.16)	(0.15)	(0.10)	(0.13)	(0.13)	(0.25)	(0.18)	(0.42)	(0.20)	(0.16)	(0.10)	(0.07)	(0.34)	(0.19)	(0.16)	(0.17)	(0.10)	(0.18)	(0.26)
Number of headlines	0.05***	0.06***	0.05***	0.05***	0.06***	0.05***	0.06***	0.05***	0.06***	0.05***	0.05***	0.07***	0.05***	0.06***	0.06***	0.06***	0.08***	0.05***	0.06***	0.05***	0.05***	0.05***	0.06***
	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)
DoS attack (t-1)	2.62***	2.69***	2.68***	2.72***	2.71***	2.71***	2.57***	2.70***	2.70***	2.72***	2.71***	2.60***	2.69***	2.63***	2.65***	2.67***	2.56***	2.72***	2.70***	2.70**	2.71***	2.68***	2.54***
	(0.55)	(0.59)	(0.57)	(0.60)	(0.61)	(0.60)	(0.52)	(0.62)	(0.50)	(0.61)	(0.61)	(0.59)	(0.60)	(0.59)	(0.61)	(0.61)	(0.49)	(0.59)	(0.60)	(0.60)	(0.60)	(0.58)	(0.56)
AIC	395.53	397.06	398.50	398.64	398.38	399.57	380.87	399.49	397.44	399.56	399.52	393.13	398.49	396.39	397.38	396.92	389.30	399.11	398.68	397.95	398.73	399.30	391.26
BIC	420.20	421.73	423.17	423.28	423.65	424.24	414.54	424.16	422.11	424.23	424.19	417.80	423.16	421.06	422.05	421.59	413.97	423.78	423.35	422.62	423.40	423.97	415.93
Log Likelihood	-193.76	-194.53	-195.25	-195.30	-195.49	-195.78	-190.94	-195.74	-194.72	-195.78	-195.76	-192.57	-195.24	-194.19	-194.69	-194.46	-190.65	-195.56	-195.34	-194.97	-195.36	-195.65	-191.63
Deviance	387.53	389.06	390.50	390.61	390.98	391.57	381.87	391.49	389.44	391.56	391.52	385.13	390.49	388.39	389.38	388.92	381.30	391.11	390.68	389.95	390.73	391.30	383.26
Num. obs.	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524	3524

Table D.4.5: Penalized logistic regression results - medium-term (t-2 – t-7) models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.85**	0.04	−0.06	0.18*	0.07	−0.15	0.06	0.12	−1.22***	0.21*	0.25	−0.68	0.25**	−0.44	0.26*	−0.24***	−0.04	0.31	−0.17	0.12	0.01
	(0.40)	(0.16)	(0.12)	(0.08)	(0.15)	(0.17)	(0.17)	(0.24)	(0.17)	(0.10)	(0.18)	(0.37)	(0.09)	(0.33)	(0.12)	(0.06)	(0.26)	(0.21)	(0.16)	(0.12)	(0.12)
DoS attack (t-1)	2.06***	2.09***	2.09***	2.05***	2.09***	2.10***	2.09***	2.10***	2.06***	2.08***	2.08***	2.07***	2.08***	2.04***	2.08***	2.07***	2.10***	2.08***	2.07***	2.09***	2.09***
	(0.36)	(0.35)	(0.35)	(0.38)	(0.35)	(0.35)	(0.35)	(0.36)	(0.34)	(0.35)	(0.34)	(0.31)	(0.35)	(0.36)	(0.34)	(0.34)	(0.35)	(0.37)	(0.35)	(0.36)	(0.35)
AIC	403.83	406.17	406.11	405.15	406.03	405.90	406.22	406.26	404.20	405.51	405.54	404.28	405.33	404.69	405.61	404.88	406.15	405.12	405.58	405.93	405.98
BIC	534.00	536.34	536.27	535.32	536.19	536.07	536.39	536.43	534.36	535.67	535.71	534.44	535.49	534.86	535.77	535.04	536.31	535.28	535.75	536.09	536.15
Log Likelihood	-180.91	-182.09	-182.05	-181.58	-182.01	-181.95	-182.11	-182.13	-181.10	-181.75	-181.77	-181.14	-181.66	-181.35	-181.80	-181.44	-182.07	-181.56	-181.79	-181.96	-181.99
Deviance	361.83	364.17	364.11	363.15	364.03	363.90	364.22	364.26	362.20	363.51	363.54	362.28	363.33	362.69	363.61	362.88	364.15	363.12	363.58	363.93	363.98
Num. obs.	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.07	−0.27	−0.35**	0.75***	0.38*	0.18	0.15	0.16	−0.12	0.30***	−0.37*	−0.21	−0.12	0.16***	0.09	0.06	−0.03	−0.25*	−0.30	0.41*	−0.50
	(0.18)	(0.25)	(0.13)	(0.19)	(0.16)	(0.22)	(0.09)	(0.15)	(0.17)	(0.08)	(0.17)	(0.17)	(0.11)	(0.04)	(0.11)	(0.19)	(0.16)	(0.10)	(0.20)	(0.19)	(0.32)
DoS attack (t-1)	2.09***	2.08***	2.07***	2.06***	2.10***	2.10***	2.08***	2.08***	2.09***	2.04***	2.07***	2.08***	2.09**	2.07***	2.09***	2.09***	2.09***	2.09***	2.06***	2.01***	2.07***
	(0.36)	(0.33)	(0.36)	(0.25)	(0.34)	(0.34)	(0.35)	(0.37)	(0.34)	(0.35)	(0.34)	(0.36)	(0.35)	(0.36)	(0.35)	(0.36)	(0.35)	(0.35)	(0.38)	(0.25)	(0.33)
AIC	406.08	404.72	405.39	399.26	406.15	405.68	406.02	405.65	405.83	405.19	405.29	405.52	405.77	405.78	406.15	406.12	406.08	405.56	405.26	402.49	404.61
BIC	536.24	534.89	535.56	529.42	536.32	535.84	536.18	535.82	535.99	535.35	535.45	535.69	535.94	535.95	536.32	536.29	536.25	535.73	535.42	532.66	534.77
Log Likelihood	-182.04	-181.36	-181.70	-178.63	-182.08	-181.84	-182.01	-181.83	-181.91	-181.59	-181.64	-181.76	-181.89	-181.89	-182.08	-182.06	-182.04	-181.78	-181.63	-180.25	-181.30
Deviance	364.08	362.72	363.39	357.26	364.15	363.68	364.02	363.65	363.83	363.19	363.29	363.52	363.77	363.78	364.15	364.12	364.08	363.56	363.26	360.49	362.61
Num. obs.	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635

Table D.4.6: Penalized logistic regression results - medium-term (t-2 – t-7) models (newspaper fixed effects). Note: Newspaper fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.90***	0.17	−0.21	−0.16	0.06	−0.02	0.44***	0.56***	−1.48***	0.01	−0.40**	−0.63**	0.14	0.35*	0.40***	0.26*	0.33***	0.57***	0.02	0.04	−0.11
	(0.23)	(0.12)	(0.21)	(0.09)	(0.17)	(0.09)	(0.11)	(0.12)	(0.16)	(0.20)	(0.14)	(0.24)	(0.13)	(0.18)	(0.10)	(0.12)	(0.09)	(0.17)	(0.13)	(0.06)	(0.15)
DoS attack (t-1)	1.55***	1.57***	1.56***	1.58***	1.57***	1.57***	1.55***	1.56***	1.56***	1.57***	1.54***	1.54***	1.58***	1.58***	1.56***	1.57**	1.54***	1.57***	1.57***	1.57***	1.57***
	(0.30)	(0.31)	(0.31)	(0.31)	(0.31)	(0.31)	(0.31)	(0.30)	(0.30)	(0.31)	(0.32)	(0.26)	(0.31)	(0.31)	(0.30)	(0.32)	(0.33)	(0.32)	(0.30)	(0.31)	(0.31)
AIC	428.61	430.47	430.24	429.97	430.57	430.85	429.17	428.93	428.36	430.67	429.39	428.83	430.49	430.84	429.51	430.62	430.54	428.02	430.86	430.62	430.32
BIC	701.34	703.20	702.96	702.70	703.30	703.58	701.89	701.66	701.08	703.40	702.12	701.56	703.21	703.56	702.24	703.35	703.27	700.75	703.58	703.35	703.05
Log Likelihood	-170.30	-171.24	-171.12	-170.98	-171.28	-171.42	-170.58	-170.46	-170.18	-171.34	-170.70	-170.41	-171.24	-171.42	-170.76	-171.31	-171.27	-170.01	-171.43	-171.31	-171.16
Deviance	340.61	342.47	342.24	341.97	342.57	342.85	341.17	340.93	340.36	342.67	341.39	340.83	342.49	342.84	341.51	342.62	342.54	340.02	342.86	342.62	342.32
Num. obs.	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.28***	0.16	−0.58***	0.86***	0.02	0.65***	0.19*	0.24	0.05	0.46**	−0.63**	0.10	−0.32***	0.06	0.09	0.24	−0.49***	−0.34	−0.40**	0.41***	0.12
	(0.07)	(0.24)	(0.16)	(0.20)	(0.25)	(0.08)	(0.07)	(0.14)	(0.10)	(0.18)	(0.24)	(0.21)	(0.07)	(0.11)	(0.13)	(0.20)	(0.15)	(0.18)	(0.16)	(0.11)	(0.11)
DoS attack (t-1)	1.56***	1.57***	1.52***	1.48***	1.57***	1.51***	1.56***	1.55***	1.57***	1.52***	1.53***	1.58***	1.55***	1.57***	1.57***	1.56***	1.57***	1.58***	1.57***	1.54***	1.58***
	(0.31)	(0.33)	(0.33)	(0.23)	(0.32)	(0.27)	(0.31)	(0.32)	(0.31)	(0.30)	(0.31)	(0.30)	(0.31)	(0.31)	(0.31)	(0.33)	(0.30)	(0.31)	(0.31)	(0.26)	(0.31)
AIC	430.59	430.80	428.87	423.46	430.92	426.52	430.24	429.86	430.71	429.21	429.17	430.85	429.03	430.62	430.73	430.60	428.98	429.81	429.50	429.46	431.17
BIC	703.32	703.53	701.59	696.19	703.65	699.25	702.97	702.59	703.44	701.94	701.89	703.58	701.76	703.35	703.46	703.32	701.70	702.54	702.23	702.19	703.89
Log Likelihood	-171.30	-171.40	-170.43	-167.73	-171.46	-169.26	-171.12	-170.93	-171.36	-170.61	-170.58	-171.42	-170.52	-171.31	-171.37	-171.30	-170.49	-170.90	-170.75	-170.73	-171.58
Deviance	342.59	342.80	340.87	335.46	342.92	338.52	342.24	341.86	342.71	341.21	341.17	342.85	341.03	342.62	342.73	342.60	340.98	341.81	341.50	341.46	343.17
Num. obs.	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635

Table D.4.7: Penalized logistic regression results - medium-term (t-2 – t-7) models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.76**	0.25*	−0.42*	−0.21*	0.26*	0.12	0.29***	0.41***	−0.37**	0.22	−0.21*	−0.48**	0.10	0.34	0.40***	0.05	0.22***	0.52**	0.15	0.02	−0.20
	(0.27)	(0.11)	(0.20)	(0.11)	(0.13)	(0.10)	(0.09)	(0.10)	(0.12)	(0.14)	(0.08)	(0.16)	(0.12)	(0.21)	(0.08)	(0.14)	(0.05)	(0.17)	(0.09)	(0.05)	(0.13)
DoS attack (t-1)	2.90***	2.96***	2.92***	2.91***	2.97***	2.95***	2.88***	2.90***	2.92***	2.95***	2.91***	2.87***	2.92**	2.93***	2.92***	2.93***	2.92***	2.85***	2.96***	2.94***	2.94***
	(0.37)	(0.39)	(0.39)	(0.38)	(0.39)	(0.38)	(0.40)	(0.37)	(0.38)	(0.39)	(0.39)	(0.35)	(0.39)	(0.38)	(0.39)	(0.38)	(0.39)	(0.43)	(0.38)	(0.39)	(0.39)
AIC	345.49	346.79	346.04	346.53	346.64	347.46	346.58	345.83	347.16	347.17	346.94	345.85	347.13	347.22	345.81	347.14	347.29	344.68	347.33	347.29	346.41
BIC	735.99	737.29	736.54	737.03	737.14	737.95	737.08	736.33	737.66	737.67	737.43	736.35	737.62	737.72	736.31	737.63	737.79	735.17	737.83	737.79	736.91
Log Likelihood	-169.75	-170.39	-170.02	-170.27	-170.32	-170.73	-170.29	-169.92	-170.58	-170.59	-170.47	-169.93	-170.56	-170.61	-169.90	-170.57	-170.65	-169.34	-170.67	-170.65	-170.21
Deviance	219.49	220.79	220.04	220.53	220.64	221.46	220.58	219.83	221.16	221.17	220.94	219.85	221.13	221.22	219.81	221.14	221.29	218.68	221.33	221.29	220.41
Num. obs.	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.31**	0.22	−0.04	0.67***	0.08	0.51***	0.25*	0.07	0.12	0.74***	−0.36*	−0.12	−0.50***	−0.05	0.21**	0.13	−0.28***	−0.20	−0.40**	0.16	−0.09
	(0.11)	(0.13)	(0.10)	(0.16)	(0.15)	(0.10)	(0.11)	(0.13)	(0.07)	(0.17)	(0.16)	(0.21)	(0.10)	(0.15)	(0.07)	(0.21)	(0.06)	(0.12)	(0.14)	(0.10)	(0.15)
DoS attack (t-1)	2.93***	2.98***	2.93***	2.72***	2.94***	2.87***	2.91***	2.92***	2.96***	2.90***	2.92***	2.96***	2.92**	2.93***	2.96***	2.92**	2.87***	2.93**	2.91**	2.90**	2.95***
	(0.38)	(0.38)	(0.39)	(0.31)	(0.38)	(0.35)	(0.39)	(0.39)	(0.38)	(0.37)	(0.39)	(0.37)	(0.36)	(0.38)	(0.40)	(0.40)	(0.38)	(0.39)	(0.39)	(0.36)	(0.38)
AIC	346.73	346.74	347.33	341.72	347.49	344.33	345.58	347.22	347.26	343.60	346.35	347.14	343.39	347.24	347.23	347.20	346.57	346.82	346.03	347.34	347.13
BIC	737.22	737.23	737.83	732.22	737.99	734.83	736.07	737.71	737.76	734.09	736.85	737.64	733.89	737.73	737.72	737.69	737.06	737.31	736.53	737.83	737.62
Log Likelihood	-170.36	-170.37	-170.66	-167.86	-170.74	-169.16	-169.79	-170.61	-170.63	-168.80	-170.18	-170.57	-168.69	-170.62	-170.61	-170.60	-170.28	-170.41	-170.02	-170.67	-170.56
Deviance	220.73	220.74	221.33	215.72	221.49	218.33	219.58	221.22	221.26	217.60	220.35	221.14	217.39	221.24	221.23	221.20	220.57	220.82	220.03	221.34	221.13
Num. obs.	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635	3635

Table D.4.8: Penalized logistic regression results - medium-term (t-2 – t-7) models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.05	−0.11	−0.42	0.36***	0.44***	−0.07	−0.25	−0.12	0.23	−0.01	0.06	−0.58***	−0.03	−5.61***	−0.23	0.08	0.40***	0.06	−0.17	0.13	0.20	−0.44	0.22
	(0.25)	(0.28)	(0.21)	(0.07)	(0.12)	(0.15)	(0.26)	(0.23)	(0.17)	(0.19)	(0.22)	(0.16)	(0.24)	(1.80)	(0.31)	(0.13)	(0.13)	(0.18)	(0.16)	(0.17)	(0.17)	(0.30)	(0.22)
Number of headlines	0.05**	0.05**	0.06***	0.05**	0.06***	0.05**	0.06***	0.05**	0.05***	0.05**	0.05**	0.07***	0.05**	0.06***	0.05***	0.05**	0.06***	0.05**	0.05**	0.05**	0.05**	0.05***	0.05**
	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)
DoS attack (t-1)	2.71***	2.71***	2.67***	2.62***	2.62***	2.71***	2.64***	2.71***	2.69***	2.71***	2.70***	2.48***	2.72***	2.44***	2.68***	2.67***	2.64***	2.72***	2.70***	2.72***	2.69***	2.64***	2.71***
	(0.59)	(0.59)	(0.58)	(0.61)	(0.51)	(0.60)	(0.57)	(0.60)	(0.59)	(0.60)	(0.60)	(0.51)	(0.59)	(0.55)	(0.60)	(0.58)	(0.58)	(0.59)	(0.60)	(0.60)	(0.59)	(0.62)	(0.59)
AIC	411.26	410.84	407.92	405.25	402.70	410.93	409.44	410.82	410.39	411.24	411.23	401.68	411.18	396.35	410.00	410.77	406.40	411.25	410.15	411.10	410.28	408.66	409.62
BIC	435.96	435.54	432.61	429.95	427.39	435.63	434.14	435.51	435.08	435.93	435.92	426.37	435.88	421.04	434.69	435.46	431.09	435.95	434.84	435.80	434.98	433.35	434.32
Log Likelihood	-201.63	-201.42	-199.96	-198.63	-197.35	-201.47	-200.72	-201.41	-201.19	-201.62	-201.61	-196.84	-201.59	-194.18	-201.00	-201.38	-199.20	-201.63	-201.07	-201.55	-201.14	-200.33	-200.81
Deviance	403.26	402.84	399.92	397.25	394.70	402.93	401.44	402.82	402.39	403.24	403.23	393.68	403.18	388.35	402.00	402.77	398.40	403.25	402.15	403.10	402.28	400.66	401.62
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.36*	0.35***	−0.30*	0.10	−0.39	0.09	0.49***	0.17	0.18	0.01	0.12	−0.57	−0.18	0.42*	0.25*	0.33***	−1.09**	−0.27	0.15	−0.35*	−0.13	0.13	−0.98***
	(0.14)	(0.10)	(0.15)	(0.15)	(0.16)	(0.15)	(0.15)	(0.17)	(0.13)	(0.22)	(0.17)	(0.43)	(0.19)	(0.19)	(0.10)	(0.10)	(0.37)	(0.21)	(0.18)	(0.18)	(0.09)	(0.15)	(0.22)
Number of headlines	0.05***	0.06***	0.05***	0.05**	0.06***	0.05**	0.06***	0.05**	0.05***	0.05***	0.05**	0.06***	0.05***	0.06***	0.05***	0.06***	0.09***	0.05**	0.05**	0.05***	0.05**	0.05**	0.06***
	(0.01)	(0.01)	(0.01)	(0.02)	(0.01)	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)
DoS attack (t-1)	2.60***	2.68***	2.66***	2.72***	2.67***	2.70***	2.60***	2.67***	2.69***	2.71***	2.71***	2.63***	2.68***	2.59***	2.63***	2.62***	2.46***	2.71***	2.71***	2.69***	2.70***	2.69***	2.53***
	(0.54)	(0.58)	(0.54)	(0.60)	(0.59)	(0.58)	(0.52)	(0.62)	(0.59)	(0.60)	(0.60)	(0.57)	(0.60)	(0.58)	(0.61)	(0.59)	(0.45)	(0.58)	(0.60)	(0.59)	(0.60)	(0.58)	(0.55)
AIC	406.21	406.91	408.54	410.79	408.53	411.38	403.12	410.26	410.35	411.26	410.99	407.27	410.35	404.35	408.83	407.94	395.35	409.19	410.86	408.84	410.53	410.95	402.07
BIC	430.90	431.60	433.24	435.46	433.23	436.08	427.81	434.95	435.04	435.96	435.69	431.96	435.04	429.05	433.50	432.63	420.05	433.88	435.56	433.53	435.22	435.64	426.77
Log Likelihood	-199.10	-199.45	-200.27	-201.38	-200.27	-201.69	-197.56	-201.13	-201.17	-201.63	-201.50	-199.63	-201.18	-198.18	-200.40	-199.97	-193.68	-200.60	-201.43	-200.42	-201.26	-201.47	-197.04
Deviance	398.21	398.91	400.54	402.77	400.53	403.38	395.12	402.26	402.35	403.26	402.99	399.27	402.35	396.35	400.81	399.94	387.35	401.19	402.86	400.84	402.53	402.95	394.07
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.4.9: Penalized logistic regression results - medium-term (14 days) models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.57	0.20	−0.11	0.29***	0.03	0.20	−0.35	0.10	−1.35**	0.09	0.24	−0.57	0.41***	−0.20	0.42*	−0.15	0.33	0.21	−0.65**	0.06	−0.10
	(0.55)	(0.23)	(0.15)	(0.08)	(0.19)	(0.15)	(0.30)	(0.29)	(0.51)	(0.17)	(0.22)	(0.65)	(0.08)	(0.25)	(0.20)	(0.22)	(0.17)	(0.17)	(0.24)	(0.21)	(0.12)
DoS attack (t-1)	2.03***	2.06***	2.06***	1.96***	2.06***	2.06***	2.05***	2.07***	2.00***	2.05***	2.05***	2.05***	2.01***	2.04***	2.06***	2.05***	2.06***	2.04***	1.96***	2.06***	2.05***
	(0.37)	(0.35)	(0.36)	(0.41)	(0.36)	(0.36)	(0.33)	(0.37)	(0.36)	(0.36)	(0.35)	(0.34)	(0.35)	(0.36)	(0.35)	(0.35)	(0.37)	(0.37)	(0.39)	(0.36)	(0.37)
AIC	411.75	412.01	412.43	409.80	412.52	412.67	411.40	412.70	411.16	412.54	412.11	411.62	410.61	412.25	411.38	411.58	412.03	412.31	409.00	412.56	412.17
BIC	542.08	542.38	542.80	540.17	542.89	543.04	541.77	543.07	541.53	542.90	542.47	541.98	540.98	542.62	541.75	542.34	542.39	542.68	539.37	542.93	542.54
Log Likelihood	-184.86	-185.00	-185.21	-183.90	-185.26	-185.34	-184.70	-185.35	-184.58	-185.27	-185.05	-184.81	-184.31	-185.12	-184.69	-184.99	-185.01	-185.15	-183.50	-185.28	-185.09
Deviance	369.72	370.01	370.43	367.80	370.52	370.67	369.40	370.70	369.16	370.54	370.11	369.62	368.61	370.25	369.38	369.98	370.03	370.31	367.00	370.56	370.17
Num. obs.	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.32*	−0.53*	−0.17**	0.51**	0.90***	−0.16	0.25*	0.00	−0.19	0.74***	−0.00	−0.19	0.07	0.15*	−0.04	−0.24	−0.37	−0.63***	−0.51**	0.47*	−0.46
	(0.15)	(0.21)	(0.06)	(0.19)	(0.27)	(0.30)	(0.11)	(0.19)	(0.12)	(0.14)	(0.06)	(0.18)	(0.10)	(0.06)	(0.15)	(0.27)	(0.22)	(0.09)	(0.17)	(0.20)	(0.34)
DoS attack (t-1)	2.05***	2.04***	2.06***	2.03***	2.00***	2.04***	2.01***	2.07***	2.05***	1.98***	2.06***	2.05***	2.06**	2.03***	2.07***	2.06***	2.06**	2.02***	2.03***	2.02***	2.04***
	(0.38)	(0.34)	(0.36)	(0.33)	(0.26)	(0.40)	(0.34)	(0.37)	(0.36)	(0.35)	(0.36)	(0.37)	(0.36)	(0.38)	(0.36)	(0.36)	(0.36)	(0.36)	(0.38)	(0.28)	(0.34)
AIC	411.92	409.39	412.56	410.98	407.27	412.12	410.97	412.49	412.15	407.53	412.96	412.22	412.47	412.26	412.49	412.02	410.88	410.34	410.98	408.34	411.36
BIC	542.28	539.75	542.93	541.34	537.64	542.48	541.33	542.85	542.52	537.90	543.32	542.59	542.83	542.63	542.85	542.38	541.25	540.71	541.35	538.71	541.73
Log Likelihood	-184.96	-183.69	-185.28	-184.49	-182.64	-185.06	-184.48	-185.24	-185.08	-182.77	-185.48	-185.11	-185.23	-185.13	-185.24	-185.01	-184.44	-184.17	-184.49	-183.17	-184.68
Deviance	369.92	367.39	370.56	368.98	365.27	370.12	368.97	370.49	370.15	365.53	370.96	370.22	370.47	370.26	370.49	370.02	368.88	368.34	368.98	366.34	369.36
Num. obs.	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670

Table D.4.10: Penalized logistic regression results - medium-term (14 days) models (newspaper fixed effects). Note: Newspaper fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.42	0.66***	−0.52*	0.00	0.16	0.09	0.08	0.98***	−0.29	−0.25	−0.48	−0.41	0.45***	1.32***	0.75***	−0.01	1.08***	0.39*	−0.57*	−0.25*	−0.35**
	(0.53)	(0.12)	(0.22)	(0.12)	(0.25)	(0.11)	(0.16)	(0.21)	(0.30)	(0.25)	(0.27)	(0.36)	(0.14)	(0.15)	(0.18)	(0.09)	(0.18)	(0.16)	(0.24)	(0.10)	(0.13)
DoS attack (t-1)	1.53***	1.51***	1.50***	1.53***	1.54***	1.54***	1.53***	1.48***	1.53***	1.55***	1.51***	1.52***	1.50***	1.51***	1.53***	1.53***	1.49***	1.50***	1.49***	1.54***	1.53***
	(0.31)	(0.32)	(0.32)	(0.33)	(0.33)	(0.32)	(0.33)	(0.30)	(0.32)	(0.32)	(0.34)	(0.30)	(0.33)	(0.33)	(0.31)	(0.32)	(0.35)	(0.32)	(0.31)	(0.32)	(0.32)
AIC	437.18	435.79	436.27	437.57	437.52	437.99	437.84	433.21	437.82	437.55	436.63	437.03	436.43	433.50	434.89	437.55	432.44	436.99	436.08	437.05	436.64
BIC	710.33	708.94	709.42	710.72	710.67	711.14	710.99	706.36	710.97	710.70	709.78	710.18	709.58	706.65	708.04	710.70	705.59	710.14	709.23	710.20	709.79
Log Likelihood	-174.59	-173.90	-174.13	-174.78	-174.76	-174.99	-174.92	-172.60	-174.91	-174.78	-174.31	-174.52	-174.22	-172.75	-173.45	-174.78	-172.22	-174.49	-174.04	-174.53	-174.32
Deviance	349.18	347.79	348.27	349.57	349.52	349.99	349.84	345.21	349.82	349.55	348.63	349.03	348.43	345.50	346.89	349.55	344.44	348.99	348.08	349.05	348.64
Num. obs.	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.38***	−0.16	−0.02	0.52**	0.76*	0.44*	0.37***	−0.07	−0.11	1.42***	−0.12	0.16	−0.05	−0.37**	−0.24	−0.15	−1.32***	−0.72***	−0.20	0.77**	0.11
	(0.06)	(0.20)	(0.08)	(0.17)	(0.35)	(0.21)	(0.09)	(0.12)	(0.10)	(0.25)	(0.09)	(0.20)	(0.08)	(0.12)	(0.24)	(0.29)	(0.16)	(0.16)	(0.16)	(0.19)	(0.09)
DoS attack (t-1)	1.54***	1.53***	1.54***	1.50***	1.53***	1.53***	1.45***	1.55***	1.53***	1.38***	1.53***	1.55***	1.53***	1.55***	1.55***	1.54***	1.50***	1.51***	1.53***	1.52***	1.54***
	(0.32)	(0.31)	(0.32)	(0.31)	(0.25)	(0.30)	(0.31)	(0.32)	(0.33)	(0.27)	(0.32)	(0.32)	(0.32)	(0.31)	(0.31)	(0.32)	(0.29)	(0.32)	(0.32)	(0.26)	(0.33)
AIC	436.94	437.24	437.87	436.14	435.52	436.33	434.28	437.44	437.66	427.23	437.84	438.09	437.59	436.31	436.78	437.55	431.03	435.67	437.19	433.83	438.29
BIC	710.09	710.39	711.02	709.29	708.67	709.48	707.43	710.59	710.81	700.38	710.99	711.24	710.74	709.46	709.93	710.70	704.18	708.82	710.34	706.98	711.44
Log Likelihood	-174.47	-174.62	-174.94	-174.07	-173.76	-174.16	-173.14	-174.72	-174.83	-169.61	-174.92	-175.05	-174.80	-174.16	-174.39	-174.77	-171.52	-173.84	-174.59	-172.91	-175.14
Deviance	348.94	349.24	349.87	348.14	347.52	348.33	346.28	349.44	349.66	339.23	349.84	350.09	349.59	348.31	348.78	349.55	343.03	347.67	349.19	345.83	350.29
Num. obs.	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670

Table D.4.11: Penalized logistic regression results - medium-term (14 days) models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.57	0.59***	−0.96***	0.20*	0.41*	−0.07	0.16	0.77***	0.02	0.40*	−0.32*	0.10	0.35**	0.55***	0.54***	−0.31**	0.65***	0.58***	−0.20	−0.16	−0.32**
	(0.46)	(0.14)	(0.18)	(0.08)	(0.16)	(0.10)	(0.15)	(0.20)	(0.12)	(0.17)	(0.15)	(0.17)	(0.10)	(0.13)	(0.12)	(0.07)	(0.13)	(0.14)	(0.16)	(0.12)	(0.12)
DoS attack (t-1)	2.92***	2.94***	2.98***	2.97***	2.98***	2.94***	2.94***	2.78***	2.95***	2.94***	2.90***	2.96***	2.89***	2.86***	2.92***	2.94***	2.86***	2.92***	2.92***	2.94***	2.94***
	(0.38)	(0.38)	(0.36)	(0.41)	(0.41)	(0.39)	(0.40)	(0.37)	(0.39)	(0.38)	(0.41)	(0.39)	(0.39)	(0.39)	(0.38)	(0.38)	(0.43)	(0.39)	(0.39)	(0.39)	(0.38)
AIC	352.84	352.12	349.58	353.33	352.47	354.05	353.87	349.86	354.20	353.15	353.29	354.12	352.97	352.93	351.76	353.00	351.14	352.04	353.43	353.48	352.45
BIC	750.15	749.43	746.89	750.64	749.78	751.36	751.18	747.17	751.51	750.46	750.60	751.43	750.27	750.24	749.07	750.31	748.45	749.35	750.74	750.79	749.75
Log Likelihood	-112.42	-112.06	-110.79	-112.67	-112.23	-113.02	-112.93	-110.93	-113.10	-112.58	-112.64	-113.06	-112.48	-112.47	-111.88	-112.50	-111.57	-112.02	-112.72	-112.74	-112.22
Deviance	224.84	224.12	221.58	225.33	224.47	226.05	225.87	221.86	226.20	225.15	225.29	226.12	224.97	224.93	223.76	225.00	223.14	224.04	225.43	225.48	224.45
Num. obs.	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.29***	−0.05	0.33***	0.25*	0.31	0.30	0.47***	−0.08	0.05	1.35***	−0.14	−0.33	−0.14*	−0.25*	−0.11	−0.05	−0.96***	−0.80***	−0.38**	0.49**	0.03
	(0.05)	(0.13)	(0.09)	(0.11)	(0.23)	(0.19)	(0.09)	(0.15)	(0.06)	(0.23)	(0.09)	(0.27)	(0.07)	(0.10)	(0.19)	(0.25)	(0.11)	(0.12)	(0.12)	(0.13)	(0.08)
DoS attack (t-1)	2.95***	2.93***	2.96***	2.88***	2.89***	2.93***	2.88***	2.95***	2.96***	2.72***	2.94***	2.98***	2.95***	2.93***	2.93***	2.94***	2.84***	2.94***	2.96***	2.83***	2.95***
	(0.37)	(0.36)	(0.38)	(0.38)	(0.32)	(0.36)	(0.37)	(0.39)	(0.38)	(0.33)	(0.39)	(0.39)	(0.38)	(0.37)	(0.29)	(0.39)	(0.37)	(0.37)	(0.38)	(0.32)	(0.39)
AIC	352.91	353.71	353.52	353.48	353.42	353.00	347.95	353.62	353.93	341.85	353.81	353.14	353.42	352.55	353.57	353.78	349.62	350.75	353.08	351.63	354.18
BIC	750.22	751.01	750.83	750.79	750.72	750.30	745.26	750.93	751.24	739.16	751.12	750.45	750.73	749.86	750.88	751.09	746.93	748.06	750.39	748.93	751.49
Log Likelihood	-112.46	-112.85	-112.76	-112.74	-112.71	-112.50	-109.98	-112.81	-112.96	-106.93	-112.91	-112.57	-112.71	-112.27	-112.79	-112.89	-110.81	-111.38	-112.54	-111.81	-113.09
Deviance	224.91	225.71	225.52	225.48	225.42	225.00	219.95	225.62	225.93	213.85	225.81	225.14	225.42	224.55	225.57	225.78	221.62	222.75	225.08	223.63	226.18
Num. obs.	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670	3670

Table D.4.12: Penalized logistic regression results - medium-term (14 days) models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.04	0.01	−0.43***	0.30***	0.25***	0.02	−0.41	−0.79*	0.23	0.27	0.03	−0.63***	−0.02	−2.20***	−0.09	0.14	0.11	−0.07	−0.17	−0.80*	0.10	−0.10	0.11
	(0.24)	(0.10)	(0.09)	(0.04)	(0.06)	(0.08)	(0.25)	(0.34)	(0.13)	(0.20)	(0.18)	(0.11)	(0.21)	(0.53)	(0.25)	(0.12)	(0.15)	(0.11)	(0.26)	(0.32)	(0.11)	(0.13)	(0.09)
Number of headlines	0.05**	0.05**	0.06**	0.06**	0.06***	0.05**	0.06***	0.05**	0.06**	0.06**	0.05**	0.07***	0.06**	0.06***	0.05**	0.05*	0.06**	0.06**	0.05**	0.05**	0.05**	0.06**	0.06**
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
Google Trends (t-1)	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00	−0.01	−0.01	−0.01
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.69***	2.70***	2.69***	2.73***	2.65***	2.70***	2.59***	2.61***	2.70***	2.66***	2.69***	2.52***	2.71***	2.58***	2.68***	2.67***	2.70***	2.69***	2.68***	2.65***	2.69***	2.69***	2.71***
	(0.58)	(0.59)	(0.59)	(0.58)	(0.56)	(0.59)	(0.55)	(0.59)	(0.59)	(0.61)	(0.59)	(0.57)	(0.59)	(0.53)	(0.60)	(0.58)	(0.60)	(0.59)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)
AIC	412.87	412.87	409.17	407.77	410.56	412.70	409.02	406.72	411.86	410.35	412.69	403.28	412.62	403.19	412.34	411.53	412.51	412.31	411.62	406.73	412.51	412.53	412.54
BIC	443.54	443.54	440.04	438.64	441.43	443.57	439.89	437.59	442.73	441.23	443.56	434.15	443.49	434.05	443.21	442.40	443.38	443.18	442.49	437.59	443.38	443.10	443.40
Log Likelihood	-201.34	-201.33	-199.59	-198.89	-200.28	-201.35	-199.51	-198.36	-200.93	-200.18	-201.34	-196.64	-201.31	-196.59	-201.17	-200.77	-201.25	-201.16	-200.81	-198.36	-201.25	-201.12	-201.27
Deviance	402.67	402.67	399.17	397.77	400.56	402.70	399.02	396.72	401.86	400.36	402.69	393.28	402.62	393.19	402.34	401.53	402.51	402.31	401.62	396.73	402.51	402.23	402.54
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.34***	0.18	−0.04	0.10	−0.08	−0.17	0.21	0.09	0.01	−0.01	0.08	−0.34*	−0.23	0.43***	0.31***	0.33***	−0.49	0.10	0.22	0.02	−0.17	−0.21	−0.70*
	(0.07)	(0.13)	(0.15)	(0.18)	(0.20)	(0.14)	(0.17)	(0.07)	(0.18)	(0.14)	(0.26)	(0.13)	(0.14)	(0.11)	(0.07)	(0.09)	(0.39)	(0.12)	(0.15)	(0.17)	(0.17)	(0.21)	(0.30)
Number of headlines	0.06***	0.06**	0.06**	0.05**	0.06**	0.06**	0.06***	0.05**	0.05**	0.05**	0.05**	0.06**	0.05**	0.06***	0.06**	0.06**	0.07***	0.06**	0.06**	0.05**	0.05**	0.06**	0.06***
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
Google Trends (t-1)	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00	−0.00	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.56***	2.66***	2.69***	2.68***	2.68***	2.72***	2.68***	2.69***	2.70***	2.70**	2.70**	2.66***	2.70***	2.61***	2.65***	2.66***	2.59***	2.69***	2.69***	2.70**	2.68**	2.71***	2.57***
	(0.58)	(0.58)	(0.59)	(0.58)	(0.60)	(0.58)	(0.57)	(0.61)	(0.60)	(0.60)	(0.59)	(0.60)	(0.60)	(0.60)	(0.61)	(0.60)	(0.53)	(0.60)	(0.60)	(0.60)	(0.59)	(0.60)	(0.56)
AIC	405.37	411.81	412.46	412.59	412.33	411.68	411.44	412.85	412.66	412.63	412.55	410.43	411.33	403.90	409.22	407.38	408.03	412.46	411.66	412.68	411.57	411.32	406.72
BIC	436.24	442.68	443.33	443.46	443.20	442.55	442.30	443.72	443.53	443.50	443.42	441.30	442.10	436.77	440.19	438.25	438.90	443.33	442.53	443.55	442.44	442.19	437.59
Log Likelihood	-197.68	-200.90	-201.23	-201.29	-201.17	-200.84	-200.72	-201.43	-201.33	-201.31	-201.28	-200.21	-200.62	-197.95	-199.66	-198.69	-199.02	-201.23	-200.83	-201.34	-200.79	-200.66	-198.36
Deviance	395.37	401.81	402.46	402.59	402.33	401.68	401.44	402.85	402.66	402.63	402.55	400.43	401.23	393.90	399.22	397.38	398.03	402.46	401.66	402.68	401.57	401.32	396.72
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.13: Penalized logistic regression results (trend) - short-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.17	0.23*	−0.36***	0.28***	−0.01	0.23***	−0.43*	−0.89**	0.10	0.37**	0.05	−0.42*	0.22*	−0.00	−0.20	−0.37**	−1.09***	0.01	−0.09	0.03	0.20**
	(0.23)	(0.10)	(0.06)	(0.04)	(0.08)	(0.04)	(0.17)	(0.28)	(0.24)	(0.14)	(0.18)	(0.20)	(0.10)	(0.20)	(0.17)	(0.13)	(0.29)	(0.12)	(0.14)	(0.09)	(0.07)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	1.89***	1.88***	1.91***	1.92***	1.89***	1.88***	1.84***	1.78***	1.90***	1.89***	1.88***	1.90***	1.85***	1.89***	1.86***	1.91***	1.82***	1.89***	1.88***	1.89***	1.85***
	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.38)	(0.42)	(0.41)	(0.40)	(0.41)	(0.40)	(0.39)	(0.41)	(0.41)	(0.40)	(0.42)	(0.40)	(0.41)	(0.40)	(0.41)
AIC	400.87	400.61	399.25	397.94	401.10	401.22	398.60	394.62	401.55	397.61	401.28	399.84	400.62	401.29	400.37	398.97	393.49	401.19	401.01	401.17	399.63
BIC	536.70	536.44	535.07	533.77	536.92	537.04	534.42	530.45	537.38	533.44	537.10	535.67	536.44	537.11	536.20	534.80	529.32	537.02	536.84	536.99	535.46
Log Likelihood	-178.44	-178.31	-177.62	-176.97	-178.55	-178.61	-177.30	-175.31	-178.78	-176.81	-178.64	-177.92	-178.31	-178.64	-178.19	-177.49	-174.75	-178.60	-178.51	-178.58	-177.82
Deviance	356.87	356.61	355.25	353.94	357.10	357.22	354.60	350.62	357.55	353.61	357.28	355.84	356.62	357.29	356.37	354.97	349.49	357.19	357.01	357.17	355.63
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.00	0.01	0.48**	0.30**	−0.16	−0.25	0.07	−0.13	−0.09	0.30	−0.06	−0.30***	0.30	0.28***	0.32**	0.10	0.28***	0.04	0.15	−0.17	−0.54**
	(0.12)	(0.12)	(0.16)	(0.09)	(0.13)	(0.26)	(0.07)	(0.20)	(0.13)	(0.28)	(0.13)	(0.09)	(0.18)	(0.02)	(0.11)	(0.18)	(0.08)	(0.14)	(0.17)	(0.21)	(0.20)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	1.89***	1.89***	1.84***	1.92***	1.92***	1.85***	1.88***	1.87***	1.89***	1.92***	1.89***	1.93***	1.88***	1.89***	1.87***	1.89***	1.87***	1.89***	1.89***	1.89***	1.87***
	(0.41)	(0.40)	(0.36)	(0.41)	(0.39)	(0.42)	(0.41)	(0.39)	(0.41)	(0.40)	(0.40)	(0.41)	(0.41)	(0.40)	(0.43)	(0.40)	(0.40)	(0.40)	(0.40)	(0.41)	(0.39)
AIC	401.17	401.23	398.52	400.41	400.93	399.64	401.41	400.66	400.88	399.79	401.29	399.73	399.45	399.98	398.61	401.35	399.98	401.25	401.29	400.55	398.70
BIC	536.99	537.06	534.35	536.23	536.76	535.46	537.24	536.48	536.81	535.61	537.12	535.56	535.28	535.81	534.43	537.18	535.81	537.07	537.11	536.37	534.53
Log Likelihood	-178.58	-178.62	-177.26	-178.20	-178.47	-177.82	-178.71	-178.33	-178.49	-177.89	-178.65	-177.87	-177.73	-177.99	-177.30	-178.68	-177.99	-178.62	-178.64	-178.27	-177.35
Deviance	357.17	357.23	354.52	356.41	356.93	355.64	357.41	356.66	356.98	355.79	357.29	355.73	355.45	355.98	354.61	357.35	355.98	357.25	357.29	356.55	354.70
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.14: Penalized logistic regression results (trend) - short-term models (newspaper fixed effects). Note: Newspaper fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.17	0.12	−0.63***	0.25**	−0.11	0.10	−0.24*	−0.73***	0.24	0.35**	−0.19	−0.30**	0.12	0.34***	−0.25	−0.16	−0.91***	0.08	−0.18	0.04	0.21
	(0.17)	(0.11)	(0.09)	(0.04)	(0.11)	(0.08)	(0.11)	(0.20)	(0.21)	(0.12)	(0.19)	(0.15)	(0.09)	(0.10)	(0.13)	(0.18)	(0.19)	(0.07)	(0.12)	(0.10)	(0.12)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	1.39***	1.39***	1.41***	1.43***	1.38***	1.36***	1.37***	1.32***	1.40***	1.43***	1.39***	1.40***	1.37***	1.41***	1.35***	1.41***	1.37***	1.38***	1.39***	1.39***	1.35***
	(0.37)	(0.37)	(0.35)	(0.35)	(0.37)	(0.37)	(0.36)	(0.36)	(0.37)	(0.37)	(0.37)	(0.37)	(0.37)	(0.38)	(0.38)	(0.35)	(0.37)	(0.36)	(0.37)	(0.36)	(0.38)
AIC	425.74	425.96	421.76	423.92	425.50	426.22	425.27	421.97	426.34	423.54	425.35	424.81	425.99	425.94	424.92	425.76	421.27	426.01	425.43	426.01	424.36
BIC	703.56	703.78	699.58	701.75	703.33	704.05	703.10	699.80	704.17	701.36	703.17	702.63	703.81	703.76	702.74	703.59	699.09	703.84	703.25	703.84	702.18
Log Likelihood	-167.87	-167.98	-165.88	-166.96	-167.75	-168.11	-167.64	-165.99	-168.17	-166.77	-167.67	-167.40	-168.00	-167.97	-167.46	-167.88	-165.63	-168.01	-167.71	-168.01	-167.18
Deviance	335.74	335.96	331.76	333.92	335.50	336.22	335.27	331.97	336.34	333.54	335.35	334.81	335.99	335.94	334.92	335.76	331.27	336.01	335.43	336.01	334.36
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.10	−0.02	0.57***	0.26***	−0.38*	−0.23	0.07	−0.03	−0.03	0.35	−0.01	−0.42***	0.33	0.16***	0.35***	0.14	0.24*	0.12	0.17	−0.40**	−0.37**
	(0.06)	(0.13)	(0.09)	(0.08)	(0.15)	(0.19)	(0.04)	(0.19)	(0.09)	(0.24)	(0.10)	(0.09)	(0.17)	(0.04)	(0.09)	(0.14)	(0.10)	(0.11)	(0.18)	(0.14)	(0.14)
Google Trends (t-1)	0.01	0.01	0.02*	0.01	0.02*	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	1.37***	1.39***	1.31***	1.42***	1.43***	1.38***	1.38***	1.38***	1.39***	1.41***	1.39***	1.45***	1.40***	1.40***	1.38***	1.39***	1.39***	1.39***	1.38***	1.37***	1.38***
	(0.37)	(0.36)	(0.33)	(0.37)	(0.35)	(0.35)	(0.37)	(0.36)	(0.37)	(0.34)	(0.37)	(0.38)	(0.38)	(0.36)	(0.37)	(0.37)	(0.36)	(0.37)	(0.37)	(0.38)	(0.35)
AIC	426.01	425.99	422.83	425.40	424.65	424.86	426.25	425.97	426.10	424.51	426.23	423.77	423.84	425.84	422.92	426.28	425.52	425.95	426.18	423.63	424.91
BIC	703.83	703.81	700.66	703.22	702.48	702.68	704.07	703.79	703.92	702.34	704.05	701.59	701.67	703.66	700.74	704.10	703.35	703.78	704.00	701.46	702.73
Log Likelihood	-168.00	-167.99	-166.42	-167.70	-167.33	-167.43	-168.13	-167.98	-168.05	-167.26	-168.11	-166.88	-166.92	-167.92	-166.46	-168.14	-167.76	-167.98	-168.09	-166.82	-167.46
Deviance	336.01	335.99	332.83	335.40	334.65	334.86	336.25	335.97	336.10	334.51	336.23	333.77	333.84	335.84	332.92	336.28	335.52	335.95	336.18	333.63	334.91
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.15: Penalized logistic regression results (trend) - short-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.47	−0.09	−0.91***	0.51***	0.01	0.02	−0.12	−0.70***	0.11	0.21*	−0.29***	−0.31**	0.09	0.26	−0.38***	0.01	−0.42***	−0.08	−0.70***	0.24	0.10
	(0.30)	(0.09)	(0.11)	(0.05)	(0.14)	(0.07)	(0.07)	(0.14)	(0.15)	(0.09)	(0.07)	(0.10)	(0.10)	(0.18)	(0.09)	(0.19)	(0.10)	(0.17)	(0.09)	(0.13)	(0.06)
Google Trends (t-1)	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02**	0.02**	0.02***	0.02**	0.02***	0.02***	0.02***	0.02***	0.02***
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
DoS attack (t-1)	2.89***	2.86***	2.86***	2.97***	2.85***	2.84***	2.84***	2.77***	2.85***	2.85***	2.86***	2.88***	2.83***	2.87***	2.82***	2.84***	2.86***	2.87***	2.90***	2.92***	2.83***
	(0.45)	(0.42)	(0.38)	(0.39)	(0.40)	(0.42)	(0.41)	(0.40)	(0.42)	(0.42)	(0.41)	(0.43)	(0.44)	(0.44)	(0.45)	(0.41)	(0.43)	(0.44)	(0.43)	(0.39)	(0.41)
AIC	347.71	349.18	341.67	345.22	349.18	349.55	349.01	346.45	349.63	348.90	348.45	347.59	349.24	349.11	347.01	349.30	348.06	349.07	345.14	348.54	348.75
BIC	749.01	750.49	742.97	746.52	750.48	750.85	750.31	747.75	750.93	750.20	749.75	748.89	750.54	750.41	748.31	750.60	749.36	750.37	746.44	749.84	750.05
Log Likelihood	-108.85	-109.59	-105.83	-107.61	-109.59	-109.77	-109.51	-108.23	-109.82	-109.45	-109.23	-108.79	-109.62	-109.56	-108.50	-109.65	-109.03	-109.53	-107.57	-109.27	-109.37
Deviance	217.71	219.18	211.67	215.22	219.18	219.55	219.01	216.45	219.63	218.90	218.45	217.59	219.24	219.11	217.01	219.30	218.06	219.07	215.14	218.54	218.75
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.13	0.27	0.59***	0.18*	−0.81***	0.20	0.44***	0.05	−0.02	0.31*	0.03	−0.58***	0.53***	0.29***	0.22**	0.23	−0.16	0.23*	0.30**	−0.43**	−0.45**
	(0.09)	(0.15)	(0.14)	(0.09)	(0.14)	(0.11)	(0.08)	(0.12)	(0.07)	(0.15)	(0.06)	(0.12)	(0.12)	(0.07)	(0.07)	(0.12)	(0.08)	(0.11)	(0.10)	(0.14)	(0.15)
Google Trends (t-1)	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
DoS attack (t-1)	2.90***	2.89***	2.69***	2.82***	2.96***	2.87***	2.94***	2.85***	2.84***	2.79***	2.84***	2.96***	2.89***	2.88***	2.80***	2.85***	2.86***	2.88***	2.87***	2.77***	2.79***
	(0.42)	(0.44)	(0.39)	(0.42)	(0.42)	(0.43)	(0.43)	(0.42)	(0.43)	(0.40)	(0.42)	(0.41)	(0.43)	(0.41)	(0.45)	(0.43)	(0.41)	(0.42)	(0.41)	(0.43)	(0.39)
AIC	349.05	348.92	347.18	348.62	344.86	348.78	347.13	349.02	349.39	348.16	349.56	345.82	342.26	347.80	348.53	349.30	348.88	348.50	348.11	347.00	348.00
BIC	750.35	750.22	748.48	749.92	746.16	750.08	748.43	750.32	750.69	749.46	750.86	747.12	743.56	749.10	749.83	750.61	750.18	749.80	749.41	748.30	749.30
Log Likelihood	-109.52	-109.46	-108.59	-109.31	-107.43	-109.39	-108.56	-109.51	-109.70	-109.08	-109.78	-107.91	-106.13	-108.90	-109.26	-109.65	-109.44	-109.25	-109.05	-108.50	-109.00
Deviance	219.05	218.92	217.18	218.62	214.86	218.78	217.13	219.02	219.39	218.16	219.56	215.82	212.26	217.80	218.53	219.30	218.88	218.50	218.11	217.00	218.00
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.16: Penalized logistic regression results (trend) - short-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.11	−0.10	−0.44*	0.28***	0.37***	−0.14	−0.16	−0.15	0.21	0.09	0.08	−0.62***	0.00	−2.78***	−0.33	0.08	0.39***	−0.01	−0.21	0.03	0.24	−0.24	0.22
	(0.23)	(0.23)	(0.19)	(0.08)	(0.08)	(0.15)	(0.20)	(0.22)	(0.16)	(0.13)	(0.20)	(0.11)	(0.22)	(0.74)	(0.28)	(0.12)	(0.11)	(0.14)	(0.19)	(0.21)	(0.13)	(0.22)	(0.16)
Number of headlines	0.05**	0.06**	0.06**	0.06***	0.06***	0.05**	0.06**	0.05**	0.06**	0.06**	0.06**	0.07***	0.06**	0.06***	0.05**	0.05**	0.06***	0.06**	0.05**	0.06**	0.05**	0.06**	0.06**
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
Google Trends (t-1)	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.70***	2.69***	2.65***	2.63***	2.63***	2.69**	2.66***	2.69***	2.68***	2.69***	2.69***	2.44***	2.70***	2.53**	2.64***	2.67***	2.63***	2.69***	2.68***	2.70**	2.68**	2.66***	2.68***
	(0.59)	(0.59)	(0.58)	(0.63)	(0.55)	(0.58)	(0.58)	(0.60)	(0.59)	(0.60)	(0.59)	(0.50)	(0.59)	(0.56)	(0.60)	(0.57)	(0.58)	(0.59)	(0.60)	(0.59)	(0.60)	(0.60)	(0.60)
AIC	412.53	412.26	409.37	400.53	406.41	411.85	411.74	412.07	412.60	412.48	412.59	402.63	412.63	403.23	410.48	412.17	407.83	412.58	411.23	412.69	411.23	411.30	411.15
BIC	443.40	443.13	440.24	440.40	437.27	442.72	442.61	442.94	442.87	443.32	443.46	433.50	443.49	434.10	441.35	443.04	438.70	443.45	442.10	443.56	442.10	442.16	442.02
Log Likelihood	-201.26	-201.13	-199.69	-199.77	-198.20	-200.93	-200.87	-201.04	-201.00	-201.23	-201.30	-196.32	-201.31	-196.61	-200.24	-201.09	-198.92	-201.29	-200.62	-201.35	-200.62	-200.65	-200.58
Deviance	402.53	402.26	399.37	399.53	396.41	401.85	401.74	402.07	402.00	402.46	402.59	392.63	402.63	393.23	400.48	402.17	397.83	402.58	401.23	402.69	401.23	401.30	401.15
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.31**	0.32*	−0.19	−0.15	−0.13	−0.04	0.49**	0.09	0.23*	−0.00	0.14	−1.01*	−0.19	0.36**	0.23**	0.25**	−0.85*	−0.13	0.21	−0.32	−0.17	0.10	−0.99**
	(0.14)	(0.13)	(0.14)	(0.14)	(0.16)	(0.18)	(0.15)	(0.14)	(0.10)	(0.19)	(0.17)	(0.43)	(0.18)	(0.12)	(0.07)	(0.09)	(0.35)	(0.20)	(0.16)	(0.18)	(0.12)	(0.16)	(0.29)
Number of headlines	0.06***	0.06***	0.06**	0.06**	0.06**	0.05**	0.06***	0.05**	0.06**	0.05**	0.05**	0.07***	0.05**	0.06***	0.06**	0.06**	0.09***	0.05**	0.06**	0.05**	0.05**	0.05**	0.06***
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
Google Trends (t-1)	−0.01	−0.00	−0.01	−0.01	−0.01	−0.01	−0.00	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00	−0.00	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.00
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.59***	2.67***	2.66***	2.70***	2.69***	2.69***	2.58***	2.69***	2.67***	2.70***	2.69***	2.58***	2.67***	2.61***	2.63***	2.63***	2.54***	2.70***	2.68***	2.68**	2.69***	2.67***	2.50***
	(0.54)	(0.59)	(0.56)	(0.59)	(0.61)	(0.60)	(0.51)	(0.61)	(0.59)	(0.60)	(0.60)	(0.58)	(0.60)	(0.58)	(0.61)	(0.60)	(0.48)	(0.59)	(0.59)	(0.60)	(0.59)	(0.57)	(0.56)
AIC	408.72	409.33	411.28	411.35	411.89	412.43	403.57	412.62	411.97	412.63	412.23	406.74	411.69	408.45	410.76	410.60	401.46	412.19	411.79	410.62	411.56	412.42	403.79
BIC	439.59	440.20	442.14	442.72	442.75	443.30	434.44	443.49	441.94	443.49	443.09	437.60	442.56	434.32	441.63	441.46	432.32	443.06	442.66	441.49	442.43	443.29	434.66
Log Likelihood	-199.36	-199.67	-200.64	-200.93	-200.94	-201.21	-196.79	-201.31	-200.54	-201.31	-201.11	-198.37	-200.85	-199.23	-200.38	-200.30	-195.73	-201.10	-200.90	-200.31	-200.78	-201.21	-196.90
Deviance	398.72	399.33	401.28	401.85	401.89	402.43	393.57	402.62	401.97	402.63	402.23	396.74	401.69	398.45	400.76	400.60	391.46	402.19	401.79	400.62	401.56	402.42	393.79
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.4.17: Penalized logistic regression results (trend) - medium-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.08	0.19	−0.16	0.17*	0.05	−0.01	−0.04	0.02	−0.84***	0.20	0.21	−0.74	0.35***	−0.59	0.39***	−0.29**	0.04	0.17	−0.34	0.06	−0.01
	(0.31)	(0.14)	(0.16)	(0.08)	(0.14)	(0.13)	(0.14)	(0.26)	(0.24)	(0.11)	(0.19)	(0.41)	(0.07)	(0.34)	(0.11)	(0.10)	(0.19)	(0.20)	(0.18)	(0.14)	(0.12)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	2.06***	2.06***	2.05***	2.02***	2.07***	2.07***	2.06***	2.07***	2.04***	2.05***	2.06***	2.04**	2.06***	2.00***	2.06***	2.03***	2.07***	2.05***	2.03***	2.06***	2.06***
	(0.37)	(0.36)	(0.37)	(0.40)	(0.36)	(0.36)	(0.36)	(0.39)	(0.36)	(0.36)	(0.36)	(0.32)	(0.36)	(0.38)	(0.35)	(0.35)	(0.36)	(0.38)	(0.37)	(0.37)	(0.36)
AIC	414.74	414.51	414.32	413.96	414.63	414.87	414.67	414.83	413.82	414.13	414.29	412.65	413.16	412.47	413.13	413.15	414.86	414.44	413.15	414.63	414.51
BIC	551.23	551.00	550.81	550.45	551.12	551.36	551.16	551.32	550.31	550.62	550.78	549.14	549.65	548.97	549.62	549.64	551.35	550.93	549.64	551.12	551.00
Log Likelihood	-185.37	-185.26	-185.16	-184.98	-185.31	-185.43	-185.34	-185.41	-184.91	-185.07	-185.15	-184.33	-184.58	-184.24	-184.57	-184.57	-185.43	-185.22	-184.57	-185.31	-185.26
Deviance	370.74	370.51	370.32	369.96	370.63	370.87	370.67	370.83	369.82	370.13	370.29	368.65	369.16	368.47	369.13	369.15	370.86	370.44	369.15	370.63	370.51
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.20	−0.32	−0.25*	0.77***	0.36	0.17	0.11	0.10	−0.19	0.57***	−0.31	−0.19	−0.02	0.15**	−0.02	0.03	−0.05	−0.28*	−0.39	0.44*	−0.56
	(0.21)	(0.20)	(0.10)	(0.21)	(0.19)	(0.28)	(0.11)	(0.14)	(0.15)	(0.10)	(0.16)	(0.16)	(0.08)	(0.04)	(0.12)	(0.18)	(0.15)	(0.12)	(0.24)	(0.18)	(0.35)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	2.06***	2.05***	2.06***	1.98***	2.08***	2.08***	2.05***	2.05***	2.05***	2.00***	2.05***	2.05***	2.06***	2.04***	2.07***	2.06***	2.07***	2.07***	2.03***	2.01***	2.04***
	(0.38)	(0.34)	(0.37)	(0.27)	(0.36)	(0.36)	(0.36)	(0.38)	(0.36)	(0.36)	(0.36)	(0.37)	(0.37)	(0.38)	(0.36)	(0.37)	(0.36)	(0.36)	(0.40)	(0.27)	(0.34)
AIC	414.35	412.92	414.32	408.13	414.90	414.27	414.70	414.38	414.09	411.01	414.15	414.18	414.59	414.39	414.63	414.69	414.62	414.02	413.42	410.56	412.95
BIC	550.84	549.42	550.81	544.62	551.40	550.77	551.19	550.87	550.58	547.50	550.64	550.67	551.08	550.88	551.11	551.18	551.18	550.51	549.92	547.05	549.44
Log Likelihood	-185.18	-184.46	-185.16	-182.06	-185.45	-185.14	-185.35	-185.19	-185.04	-183.50	-185.08	-185.09	-185.30	-185.19	-185.31	-185.34	-185.31	-185.01	-184.71	-183.28	-184.47
Deviance	370.35	368.92	370.32	364.13	370.90	370.27	370.70	370.38	370.09	367.01	370.15	370.18	370.59	370.39	370.61	370.69	370.62	370.02	369.42	366.56	368.95
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.18: Penalized logistic regression results (trend) - medium-term models (newspaper fixed effects). Note: Newspaper fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.05	0.27*	−0.52	−0.28**	−0.00	0.11	0.38***	0.55***	−0.48*	−0.05	−0.59***	−0.69*	0.19	0.25	0.64***	0.23**	0.52***	0.36**	−0.35	−0.05	−0.12
	(0.18)	(0.11)	(0.29)	(0.09)	(0.15)	(0.10)	(0.08)	(0.12)	(0.20)	(0.21)	(0.17)	(0.31)	(0.15)	(0.16)	(0.12)	(0.09)	(0.07)	(0.14)	(0.20)	(0.09)	(0.14)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	1.54***	1.53***	1.49***	1.56***	1.53***	1.53***	1.52***	1.55***	1.53***	1.54***	1.48***	1.49***	1.55***	1.54***	1.54***	1.54***	1.52***	1.52***	1.51***	1.54***	1.54***
	(0.33)	(0.33)	(0.33)	(0.32)	(0.33)	(0.33)	(0.33)	(0.32)	(0.32)	(0.33)	(0.35)	(0.27)	(0.32)	(0.33)	(0.31)	(0.33)	(0.34)	(0.33)	(0.32)	(0.32)	(0.32)
AIC	439.58	438.82	437.59	437.94	439.20	439.48	438.27	437.88	439.02	439.30	437.00	437.23	439.01	439.58	435.84	439.26	438.03	438.34	438.35	439.12	438.90
BIC	718.77	718.01	716.78	717.12	718.38	718.67	717.46	717.06	718.21	718.48	716.18	716.41	718.20	718.77	715.03	718.45	717.22	717.53	717.53	718.30	718.08
Log Likelihood	-174.79	-174.41	-173.80	-173.97	-174.60	-174.74	-174.14	-173.94	-174.51	-174.65	-173.50	-173.61	-174.51	-174.79	-172.92	-174.63	-174.02	-174.17	-174.17	-174.56	-174.45
Deviance	349.58	348.82	347.59	347.94	349.20	349.48	348.27	347.88	349.02	349.30	347.00	347.23	349.01	349.58	345.84	349.26	348.03	348.34	348.35	349.12	348.90
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.40***	0.08	−0.39***	0.85***	−0.09	0.73***	0.14	0.12	0.03	0.96***	−0.45*	0.10	−0.24***	−0.23*	−0.12	0.20	−0.53***	−0.24	−0.49*	0.47***	0.11
	(0.08)	(0.24)	(0.12)	(0.20)	(0.27)	(0.09)	(0.10)	(0.09)	(0.11)	(0.21)	(0.18)	(0.21)	(0.07)	(0.09)	(0.20)	(0.20)	(0.12)	(0.19)	(0.20)	(0.11)	(0.12)
Google Trends (t-1)	0.01	0.01	0.01	0.01	0.01	0.02*	0.01	0.01	0.01	0.02	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	1.53***	1.53***	1.51***	1.46***	1.53***	1.51***	1.52***	1.51***	1.53***	1.44***	1.51***	1.54***	1.51***	1.54***	1.55***	1.52***	1.54***	1.54***	1.53***	1.53***	1.54***
	(0.32)	(0.34)	(0.34)	(0.24)	(0.35)	(0.29)	(0.33)	(0.33)	(0.33)	(0.30)	(0.33)	(0.32)	(0.33)	(0.32)	(0.31)	(0.34)	(0.31)	(0.32)	(0.33)	(0.28)	(0.33)
AIC	437.98	439.40	438.41	432.38	439.46	433.95	439.05	438.88	439.34	433.15	438.37	439.49	438.34	438.47	438.89	439.29	437.40	438.81	437.73	437.62	439.84
BIC	717.17	718.59	717.59	711.57	718.65	713.13	718.23	718.06	718.53	712.34	717.56	718.68	717.52	717.65	718.08	718.48	716.59	718.00	716.92	716.81	719.03
Log Likelihood	-173.99	-174.70	-174.20	-171.19	-174.73	-171.97	-174.52	-174.44	-174.67	-171.58	-174.18	-174.75	-174.17	-174.23	-174.45	-174.65	-173.70	-174.41	-173.87	-173.81	-174.92
Deviance	347.98	349.40	348.41	342.38	349.46	343.95	349.05	348.88	349.34	343.15	348.37	349.49	348.34	348.47	348.89	349.29	347.40	348.81	347.73	347.62	349.84
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.19: Penalized logistic regression results (trend) - medium-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.02	0.25*	−0.81***	−0.30***	0.18	0.11	0.39***	0.58***	−0.10	0.02	−0.41***	−0.48**	0.12	0.04	0.47***	−0.02	0.34**	0.42*	−0.03	0.03	−0.18
	(0.22)	(0.13)	(0.24)	(0.04)	(0.12)	(0.11)	(0.10)	(0.12)	(0.11)	(0.17)	(0.09)	(0.16)	(0.12)	(0.23)	(0.09)	(0.10)	(0.06)	(0.16)	(0.11)	(0.07)	(0.14)
Google Trends (t-1)	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
DoS attack (t-1)	2.96***	2.98***	2.94***	2.93***	2.99***	2.97***	2.90***	2.92***	2.96***	2.96***	2.91***	2.89***	2.94***	2.96***	2.97***	2.95***	2.93***	2.91***	2.96***	2.96***	2.96***
	(0.39)	(0.39)	(0.37)	(0.37)	(0.41)	(0.38)	(0.41)	(0.37)	(0.39)	(0.38)	(0.39)	(0.34)	(0.40)	(0.39)	(0.38)	(0.38)	(0.40)	(0.42)	(0.39)	(0.39)	(0.39)
AIC	353.63	353.05	349.92	352.29	353.30	353.58	352.10	350.96	353.80	353.69	352.54	352.22	353.40	353.65	350.85	353.38	352.79	352.11	353.53	353.60	352.76
BIC	756.90	756.32	753.19	755.56	756.57	756.85	755.37	754.23	757.07	756.95	755.80	755.49	756.67	756.92	754.12	756.64	756.06	755.38	756.79	756.86	756.03
Log Likelihood	-111.82	-111.53	-109.96	-111.14	-111.65	-111.79	-111.05	-110.48	-111.90	-111.84	-111.27	-111.11	-111.70	-111.83	-110.43	-111.69	-111.40	-111.06	-111.76	-111.80	-111.38
Deviance	223.63	223.05	219.92	222.29	223.30	223.58	222.10	220.96	223.80	223.69	222.54	222.22	223.40	223.65	220.85	223.38	222.79	222.11	223.53	223.60	222.76
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.35***	0.18	0.03	0.59***	−0.06	0.59***	0.27*	0.20*	0.11*	0.98***	−0.75***	−0.14	−0.45***	−0.21	0.00	0.15	−0.50***	−0.08	−0.46**	0.24*	−0.06
	(0.06)	(0.13)	(0.09)	(0.14)	(0.16)	(0.08)	(0.12)	(0.10)	(0.05)	(0.19)	(0.20)	(0.23)	(0.11)	(0.13)	(0.11)	(0.20)	(0.06)	(0.14)	(0.16)	(0.10)	(0.13)
Google Trends (t-1)	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***	0.02***
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
DoS attack (t-1)	2.95***	2.99***	2.96***	2.76***	2.96***	2.89***	2.95***	2.92***	2.98***	2.85***	2.93***	2.98***	2.96***	2.97***	2.95***	2.94***	2.86***	2.96***	2.95***	2.92***	2.97***
	(0.37)	(0.38)	(0.39)	(0.30)	(0.39)	(0.34)	(0.39)	(0.40)	(0.38)	(0.36)	(0.39)	(0.38)	(0.37)	(0.37)	(0.39)	(0.41)	(0.38)	(0.39)	(0.40)	(0.35)	(0.39)
AIC	351.98	353.36	353.63	348.92	353.75	349.78	351.65	353.00	353.62	346.40	351.42	353.39	350.40	352.37	353.56	353.51	351.82	353.53	352.12	353.08	353.56
BIC	755.25	756.63	756.90	752.19	757.02	753.05	754.92	756.26	756.89	749.66	754.69	756.66	753.67	755.64	756.83	756.78	755.09	756.80	755.39	756.35	756.83
Log Likelihood	-110.99	-111.68	-111.82	-109.46	-111.87	-109.89	-110.83	-111.50	-111.81	-108.20	-110.71	-111.70	-110.20	-111.18	-111.78	-111.75	-110.91	-111.76	-111.06	-111.54	-111.78
Deviance	221.98	223.36	223.63	218.92	223.75	219.78	221.65	223.00	223.62	216.40	221.42	223.39	220.40	222.37	223.56	223.51	221.82	223.53	222.12	223.08	223.56
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.20: Penalized logistic regression results (trend) - medium-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.04	0.15	−0.07	0.28	0.36**	0.16	−0.43**	−0.27*	0.47*	0.14	−0.05	−0.48**	−0.09	0.13	0.03	0.16	0.09	−0.10	−0.31***	0.15	0.14	0.09	0.31**
	(0.17)	(0.14)	(0.17)	(0.15)	(0.13)	(0.10)	(0.14)	(0.11)	(0.19)	(0.21)	(0.20)	(0.17)	(0.10)	(0.16)	(0.12)	(0.13)	(0.20)	(0.13)	(0.08)	(0.09)	(0.12)	(0.11)	(0.16)
Number of headlines	0.03**	0.02*	0.03***	0.02**	0.02**	0.02**	0.03***	0.03***	0.02***	0.02***	0.03**	0.04***	0.03**	0.02**	0.02**	0.02**	0.02**	0.03***	0.03***	0.02**	0.02**	0.02**	0.02**
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	2.73***	2.70***	2.72***	2.78***	2.62***	2.70***	2.65***	2.67***	2.67***	2.70***	2.73***	2.59***	2.72***	2.74***	2.70***	2.72***	2.71***	2.70***	2.71***	2.71***	2.72***	2.72***	2.51***
	(0.58)	(0.59)	(0.60)	(0.56)	(0.52)	(0.59)	(0.54)	(0.57)	(0.51)	(0.60)	(0.58)	(0.55)	(0.60)	(0.61)	(0.58)	(0.61)	(0.60)	(0.60)	(0.58)	(0.58)	(0.59)	(0.60)	(0.52)
AIC	411.34	410.65	411.17	407.69	404.73	410.41	405.87	408.76	401.40	410.66	411.26	404.46	411.01	410.85	411.34	410.46	411.14	410.90	407.98	410.59	410.60	411.12	399.91
BIC	436.03	435.35	435.87	432.39	429.43	435.11	430.56	433.46	426.09	435.35	435.96	429.16	435.71	435.55	436.04	435.15	435.84	435.60	432.67	435.28	435.29	435.81	424.60
Log Likelihood	-201.67	-201.33	-201.59	-199.85	-198.37	-201.21	-198.93	-200.38	-196.70	-201.33	-201.63	-198.23	-201.51	-201.43	-201.67	-201.23	-201.57	-201.45	-199.99	-201.29	-201.30	-201.56	-195.95
Deviance	403.34	402.65	403.17	399.69	396.73	402.41	397.87	400.76	393.40	402.66	403.26	396.46	403.01	402.85	403.34	402.46	403.14	402.90	399.98	402.59	402.60	403.12	391.91
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies	
Topic	0.22	−0.10	0.17	0.13	−0.06	0.16	−0.03	−0.27	0.03	0.09	−0.21***	0.05	0.50**	0.31**	0.46***	−0.42	0.05	0.21	0.20	−0.24	0.01	−0.40*	
	(0.13)	(0.10)	(0.16)	(0.13)	(0.13)	(0.14)	(0.06)	(0.18)	(0.19)	(0.26)	(0.05)	(0.12)	(0.19)	(0.11)	(0.12)	(0.26)	(0.09)	(0.22)	(0.11)	(0.14)	(0.16)	(0.16)	
Number of headlines	0.02**	0.03***	0.02**	0.02**	0.03**	0.02***	0.03***	0.03**	0.03**	0.02**	0.03***	0.02*	0.02***	0.02**	0.02**	0.04***	0.02**	0.02**	0.02**	0.03***	0.03**	0.03***	
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	
DoS attack (t-1)	2.69***	2.66***	2.68***	2.70***	2.74***	2.71***	2.72***	2.68**	2.72***	2.71***	2.65***	2.71***	2.49**	2.61***	2.66***	2.60***	2.71***	2.71***	2.69***	2.71***	2.71***	2.56**	
	(0.57)	(0.56)	(0.58)	(0.59)	(0.55)	(0.57)	(0.59)	(0.56)	(0.59)	(0.60)	(0.58)	(0.59)	(0.60)	(0.59)	(0.59)	(0.53)	(0.60)	(0.60)	(0.59)	(0.58)	(0.59)	(0.53)	
AIC	409.64	410.62	410.31	410.82	411.12	410.37	411.31	408.99	411.38	411.21	409.46	411.33	399.28	406.87	400.51	406.37	411.33	409.85	409.95	409.78	411.40	405.97	
BIC	434.33	435.31	435.00	435.51	435.81	435.07	436.00	433.68	436.07	435.90	434.16	436.03	423.98	431.57	425.20	431.06	436.02	434.54	434.64	434.47	436.10	430.67	
Log Likelihood	-200.82	-201.31	-201.15	-201.41	-201.56	-201.19	-201.65	-200.49	-201.69	-201.60	-200.73	-201.67	-195.64	-199.44	-196.25	-199.18	-201.66	-200.92	-200.97	-200.89	-201.70	-198.99	
Deviance	401.64	402.62	402.31	402.82	403.12	402.37	403.31	400.99	403.38	403.21	401.46	403.33	391.28	398.87	392.51	398.37	403.33	401.85	401.95	401.78	403.40	397.97	
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	

Table D.4.21: Penalized logistic regression results (maximum proportion) - short-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.26*	0.21*	−0.10	0.16	0.11	0.18***	−0.42***	−0.35**	0.04	0.07	−0.16	−0.23	−0.04	0.11	−0.02	−0.21*	−0.04	−0.41***	−0.03	0.10	0.01	0.29
	(0.10)	(0.10)	(0.15)	(0.12)	(0.09)	(0.05)	(0.11)	(0.13)	(0.16)	(0.20)	(0.15)	(0.14)	(0.08)	(0.14)	(0.09)	(0.09)	(0.13)	(0.06)	(0.08)	(0.13)	(0.08)	(0.17)
DoS attack (t-1)	1.93***	1.85***	1.89***	1.92***	1.89***	1.87***	1.85***	1.81***	1.90***	1.89***	1.92**	1.90***	1.89***	1.90***	1.88***	1.91***	1.88***	1.87***	1.89***	1.89***	1.89***	1.82***
	(0.41)	(0.38)	(0.40)	(0.41)	(0.39)	(0.40)	(0.39)	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.41)	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.40)	(0.39)
AIC	398.16	397.85	398.72	397.96	398.61	397.99	393.84	395.01	399.00	398.96	398.10	397.88	398.97	398.75	399.04	397.96	398.94	393.19	399.02	398.66	399.06	396.06
BIC	527.81	527.50	528.37	527.61	528.26	527.64	523.49	524.66	528.66	528.61	527.75	527.53	528.62	528.40	528.69	527.61	528.59	522.84	528.67	528.31	528.71	525.71
Log Likelihood	-178.08	-177.92	-178.36	-177.98	-178.30	-178.00	-175.92	-176.51	-178.50	-178.48	-178.05	-177.94	-178.48	-178.37	-178.52	-177.98	-178.47	-175.60	-178.51	-178.33	-178.53	-177.03
Deviance	356.16	355.85	356.72	355.96	356.61	355.99	351.84	353.01	357.00	356.96	356.10	355.88	356.97	356.75	357.04	355.96	356.94	351.19	357.02	356.66	357.06	354.06
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies	
Topic	0.00	−0.08	0.31***	0.18	−0.02	−0.28	−0.07	−0.33*	−0.14	0.25	−0.02	−0.06	0.25	0.09	0.28*	−0.04	0.00	0.03	0.13	0.00	−0.29*	
	(0.14)	(0.12)	(0.09)	(0.12)	(0.14)	(0.18)	(0.08)	(0.17)	(0.14)	(0.20)	(0.08)	(0.07)	(0.16)	(0.09)	(0.13)	(0.13)	(0.07)	(0.13)	(0.12)	(0.11)	(0.13)	
DoS attack (t-1)	1.89***	1.86***	1.87***	1.92***	1.90***	1.83***	1.90***	1.85***	1.87***	1.88***	1.88***	1.89***	1.83***	1.87***	1.87***	1.89**	1.89**	1.89***	1.88***	1.89***	1.84***	
	(0.40)	(0.39)	(0.39)	(0.42)	(0.37)	(0.43)	(0.40)	(0.39)	(0.41)	(0.40)	(0.40)	(0.40)	(0.44)	(0.40)	(0.43)	(0.40)	(0.40)	(0.40)	(0.40)	(0.41)	(0.38)	
AIC	399.08	398.63	396.34	397.80	399.08	396.44	398.70	395.77	398.39	397.60	399.06	398.89	397.08	398.72	395.77	399.03	399.08	399.09	398.67	399.08	396.53	
BIC	528.73	528.28	525.99	527.45	528.73	526.10	528.35	525.42	528.04	527.25	528.71	528.54	526.73	528.38	525.42	528.68	528.73	528.74	528.32	528.74	526.18	
Log Likelihood	-178.54	-178.31	-177.17	-177.90	-178.54	-177.22	-178.35	-176.89	-178.19	-177.80	-178.53	-178.45	-177.54	-178.36	-176.88	-178.52	-178.54	-178.54	-178.33	-178.54	-177.27	
Deviance	357.08	356.63	354.34	355.80	357.08	354.44	356.70	353.77	356.39	355.60	357.06	356.89	355.08	356.72	353.77	357.03	357.08	357.09	356.67	357.08	354.53	
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	

Table D.4.22: Penalized logistic regression results (maximum proportion) - short-term models (newspaper fixed effects). Note: Newspaper fixed are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.28*	0.16	−0.22	0.12	0.09	0.19**	−0.33***	−0.24**	0.03	−0.05	−0.36*	−0.16	−0.07	0.26*	−0.03	−0.11	−0.08	−0.33***	0.03	0.07	0.03	0.29
	(0.12)	(0.10)	(0.15)	(0.12)	(0.10)	(0.07)	(0.06)	(0.08)	(0.16)	(0.16)	(0.14)	(0.16)	(0.07)	(0.13)	(0.09)	(0.08)	(0.11)	(0.05)	(0.11)	(0.13)	(0.09)	(0.16)
DoS attack (t-1)	1.43***	1.37***	1.39***	1.42***	1.39***	1.35***	1.37***	1.34***	1.39***	1.37***	1.43***	1.39***	1.38***	1.39**	1.38***	1.40***	1.38***	1.42***	1.38***	1.39***	1.39***	1.34***
	(0.37)	(0.35)	(0.35)	(0.37)	(0.35)	(0.36)	(0.36)	(0.35)	(0.37)	(0.37)	(0.37)	(0.36)	(0.36)	(0.38)	(0.36)	(0.36)	(0.37)	(0.35)	(0.37)	(0.36)	(0.36)	(0.36)
AIC	421.48	423.96	423.15	424.08	424.25	423.42	421.66	422.82	424.51	424.50	421.18	423.94	424.27	422.95	424.50	424.29	424.25	421.08	424.54	424.36	424.50	421.86
BIC	695.13	695.61	694.80	695.73	695.90	695.07	693.31	694.47	696.16	696.15	692.83	695.59	695.92	694.60	696.15	695.94	695.90	692.73	696.19	696.01	696.15	693.51
Log Likelihood	-167.74	-167.98	-167.58	-168.04	-168.13	-167.71	-166.83	-167.41	-168.26	-168.25	-166.59	-167.97	-168.14	-167.48	-168.25	-168.15	-168.12	-166.54	-168.27	-168.18	-168.25	-166.93
Deviance	335.48	335.96	335.15	336.08	336.25	335.42	333.66	334.82	336.51	336.50	333.18	335.94	336.27	334.95	336.50	336.29	336.25	333.08	336.54	336.36	336.50	333.86
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.13	−0.07	0.29***	0.16	−0.08	−0.29*	−0.09	−0.29*	−0.17	0.26*	0.06	−0.05	0.26*	−0.01	0.39***	−0.04	−0.06	0.03	0.17	−0.09	−0.24**
	(0.14)	(0.11)	(0.05)	(0.13)	(0.12)	(0.14)	(0.05)	(0.12)	(0.11)	(0.13)	(0.04)	(0.06)	(0.13)	(0.08)	(0.09)	(0.10)	(0.06)	(0.11)	(0.11)	(0.06)	(0.09)	
DoS attack (t-1)	1.37***	1.36***	1.35***	1.43***	1.41***	1.36***	1.39***	1.37***	1.37***	1.38***	1.39***	1.39***	1.36***	1.39***	1.39***	1.39***	1.39**	1.39***	1.35***	1.37***	1.35***	
	(0.36)	(0.34)	(0.35)	(0.38)	(0.34)	(0.35)	(0.36)	(0.36)	(0.38)	(0.35)	(0.36)	(0.37)	(0.40)	(0.36)	(0.37)	(0.36)	(0.36)	(0.36)	(0.35)	(0.37)	(0.34)	
AIC	424.23	424.18	422.32	423.65	424.37	422.15	424.01	422.31	423.69	423.27	424.54	424.49	422.43	424.48	420.00	424.51	424.43	424.51	423.63	424.23	422.82	
BIC	695.88	695.83	693.97	695.30	696.02	693.80	695.66	693.96	695.34	694.92	696.19	696.14	694.08	696.13	691.65	696.16	696.08	696.16	695.28	695.88	694.47	
Log Likelihood	-168.11	-168.09	-167.16	-167.83	-168.18	-167.08	-168.01	-167.15	-167.84	-167.63	-168.27	-168.24	-167.21	-168.24	-166.00	-168.25	-168.21	-168.25	-167.81	-168.12	-167.41	
Deviance	336.23	336.18	334.32	335.65	336.37	334.15	336.01	334.31	335.69	335.27	336.54	336.49	334.43	336.48	332.00	336.51	336.43	336.51	335.63	336.23	334.82	
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	

Table D.4.23: Penalized logistic regression results (maximum proportion) - short-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.28*	−0.04	−0.41***	0.21*	0.27*	0.13	−0.49***	−0.24*	0.06	−0.12	−0.31**	−0.33**	0.01	0.25	−0.07	0.01	−0.12	0.03	−0.05	−0.13	0.12	0.18
	(0.11)	(0.08)	(0.07)	(0.10)	(0.11)	(0.11)	(0.10)	(0.10)	(0.17)	(0.12)	(0.07)	(0.13)	(0.08)	(0.16)	(0.11)	(0.10)	(0.15)	(0.07)	(0.07)	(0.10)	(0.07)	(0.15)
DoS attack (t-1)	2.78***	2.84***	2.83***	2.95***	2.94***	2.81***	2.93***	2.78***	2.83***	2.80***	2.78***	2.82***	2.82***	2.85***	2.81***	2.83***	2.84***	2.83***	2.83***	2.82***	2.84***	2.81***
	(0.42)	(0.41)	(0.37)	(0.40)	(0.40)	(0.41)	(0.40)	(0.38)	(0.43)	(0.42)	(0.43)	(0.42)	(0.42)	(0.48)	(0.42)	(0.42)	(0.39)	(0.42)	(0.43)	(0.41)	(0.41)	(0.39)
AIC	348.37	349.25	344.75	348.12	347.01	348.94	343.93	347.99	349.26	348.95	347.59	347.11	349.29	347.93	349.08	349.23	348.80	349.29	349.19	348.75	348.89	348.54
BIC	743.50	744.38	739.88	743.25	742.14	744.07	739.06	743.12	744.39	744.08	742.72	742.24	744.41	743.06	744.21	744.36	743.92	744.42	744.32	743.88	744.01	743.67
Log Likelihood	-110.19	-110.63	-108.38	-110.06	-109.51	-110.47	-107.96	-109.99	-110.63	-110.47	-109.80	-109.56	-110.64	-109.97	-110.54	-110.62	-110.40	-110.65	-110.59	-110.37	-110.44	-110.27
Deviance	220.37	221.25	216.75	220.12	219.01	220.94	215.93	219.99	221.26	220.95	219.59	219.11	221.29	219.93	221.08	221.23	220.80	221.29	221.19	220.75	220.89	220.54
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.03	0.09	0.24	0.18	−0.30**	−0.03	0.08	−0.23*	−0.19	0.29	0.02	−0.10	0.39***	0.17	0.34***	0.01	−0.31***	0.17	0.31**	−0.00	−0.10	
	(0.12)	(0.15)	(0.12)	(0.10)	(0.12)	(0.15)	(0.06)	(0.11)	(0.11)	(0.15)	(0.05)	(0.07)	(0.09)	(0.10)	(0.10)	(0.15)	(0.07)	(0.15)	(0.12)	(0.08)	(0.11)	
DoS attack (t-1)	2.82***	2.85***	2.75***	2.76***	2.91***	2.81***	2.85***	2.76***	2.86***	2.77***	2.81***	2.84***	2.84***	2.84***	2.81***	2.82***	2.85***	2.87***	2.85***	2.82***	2.76***	
	(0.41)	(0.41)	(0.43)	(0.40)	(0.41)	(0.45)	(0.41)	(0.39)	(0.42)	(0.39)	(0.41)	(0.41)	(0.47)	(0.42)	(0.43)	(0.42)	(0.37)	(0.43)	(0.41)	(0.43)	(0.40)	
AIC	349.23	349.07	348.22	348.12	347.61	349.18	348.95	347.85	348.47	348.08	349.34	349.08	344.47	348.28	346.34	349.30	346.88	348.57	346.38	349.36	349.12	
BIC	744.36	744.20	743.34	743.25	742.74	744.31	744.08	742.97	743.60	743.21	744.47	744.21	739.59	743.41	741.46	744.43	742.00	743.69	741.51	744.49	744.25	
Log Likelihood	-110.62	-110.54	-110.11	-110.06	-109.81	-110.59	-110.48	-109.92	-110.24	-110.04	-110.67	-110.54	-108.23	-110.14	-109.17	-110.65	-109.44	-110.28	-109.19	-110.68	-110.56	
Deviance	221.23	221.07	220.22	220.12	219.61	221.18	220.95	219.85	220.47	220.08	221.34	221.08	216.47	220.28	218.34	221.30	218.88	220.57	218.38	221.36	221.12	
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	

Table D.4.24: Penalized logistic regression results (maximum proportion) - short-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.34	0.38	−0.13	0.33	0.36*	0.04	0.02	0.10	0.46	0.47*	0.36	−0.21	0.18	−0.26	0.02	0.50**	0.32	0.28*	0.03	0.33	0.02	0.10	0.52*
	(0.25)	(0.35)	(0.27)	(0.22)	(0.15)	(0.19)	(0.21)	(0.13)	(0.28)	(0.22)	(0.20)	(0.26)	(0.18)	(0.23)	(0.17)	(0.15)	(0.20)	(0.13)	(0.16)	(0.21)	(0.19)	(0.29)	(0.23)
Number of headlines	0.02	0.02	0.03***	0.02*	0.02***	0.02**	0.02*	0.02**	0.02***	0.02**	0.02*	0.03**	0.02**	0.03***	0.02*	0.02*	0.02**	0.02**	0.02**	0.02*	0.03**	0.02*	0.02*
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	2.72***	2.64***	2.73***	2.73***	2.64***	2.71***	2.72***	2.71***	2.56***	2.58***	2.66***	2.68***	2.70***	2.68***	2.71***	2.60***	2.69***	2.68***	2.72***	2.67***	2.72***	2.72***	2.58***
	(0.60)	(0.61)	(0.59)	(0.56)	(0.57)	(0.59)	(0.62)	(0.59)	(0.60)	(0.54)	(0.55)	(0.60)	(0.57)	(0.63)	(0.57)	(0.51)	(0.62)	(0.58)	(0.60)	(0.57)	(0.60)	(0.59)	(0.51)
AIC	409.31	407.79	410.92	407.99	406.93	411.34	411.38	411.69	404.94	405.94	407.27	410.48	410.25	409.78	411.36	404.28	408.89	408.78	411.35	407.88	411.37	411.06	404.67
BIC	434.00	432.48	435.61	432.69	431.62	436.04	436.07	435.79	429.63	430.63	431.97	435.17	434.94	434.47	436.06	428.98	433.58	433.47	436.05	432.58	436.06	435.75	429.36
Log Likelihood	-200.65	-199.89	-201.46	-200.00	-199.46	-201.67	-201.69	-201.55	-198.47	-198.97	-199.64	-201.24	-201.12	-200.89	-201.68	-198.14	-200.44	-200.39	-201.68	-199.94	-201.68	-201.53	-198.33
Deviance	401.31	399.79	402.92	399.99	398.93	403.34	403.38	403.09	396.94	397.94	399.27	402.48	402.25	401.78	403.36	396.28	400.89	400.78	403.35	399.88	403.37	403.06	396.67
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.29	0.13	0.02	0.23	0.09	0.33	0.20	0.10	0.32*	0.32	−0.27*	0.14	0.37*	0.45**	0.31**	−0.49*	0.03	0.28	0.10	0.02	0.00	−0.32
	(0.23)	(0.15)	(0.10)	(0.21)	(0.16)	(0.24)	(0.20)	(0.13)	(0.14)	(0.18)	(0.12)	(0.11)	(0.18)	(0.15)	(0.08)	(0.24)	(0.18)	(0.26)	(0.16)	(0.14)	(0.25)	(0.17)
Number of headlines	0.02*	0.02***	0.03**	0.02*	0.02**	0.02*	0.02***	0.02**	0.02**	0.02	0.03***	0.02*	0.02**	0.02***	0.02**	0.04***	0.02**	0.02**	0.02**	0.03**	0.03***	0.03**
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
DoS attack (t-1)	2.69***	2.71***	2.71***	2.70***	2.71***	2.67***	2.71***	2.72***	2.68***	2.68***	2.67***	2.71***	2.62***	2.51***	2.61***	2.64***	2.72***	2.70***	2.71***	2.71***	2.72***	2.65***
	(0.56)	(0.62)	(0.58)	(0.57)	(0.58)	(0.52)	(0.61)	(0.60)	(0.59)	(0.56)	(0.58)	(0.60)	(0.57)	(0.63)	(0.61)	(0.55)	(0.59)	(0.60)	(0.59)	(0.59)	(0.60)	(0.60)
AIC	408.89	410.64	411.37	410.16	411.19	408.24	410.20	411.10	408.42	408.79	408.66	410.83	407.32	403.70	408.18	407.08	411.34	409.67	411.12	411.42	411.38	408.33
BIC	433.58	435.33	436.06	434.86	435.89	432.93	434.89	435.79	433.12	433.49	433.36	435.52	432.01	428.40	432.88	431.78	436.04	434.36	435.82	436.11	436.07	433.02
Log Likelihood	-200.45	-201.32	-201.68	-201.08	-201.60	-200.12	-201.10	-201.55	-200.21	-200.40	-200.33	-201.41	-199.66	-197.85	-200.09	-199.54	-201.67	-200.83	-201.56	-201.71	-201.69	-200.17
Deviance	400.89	402.64	403.37	402.16	403.19	400.24	402.20	403.10	400.42	400.79	400.66	402.83	399.32	395.70	400.18	399.08	403.34	401.67	403.12	403.42	403.38	400.33
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.4.25: Penalized logistic regression results (maximum proportion) - medium-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.25	0.38	−0.12	0.12	−0.17	−0.11	−0.15	0.06	−0.75**	0.35*	0.30**	−0.03	0.21	−0.34	0.21	0.11	0.29**	−0.27*	0.07	−0.17	−0.36***	−0.01
	(0.27)	(0.27)	(0.24)	(0.11)	(0.18)	(0.10)	(0.14)	(0.14)	(0.26)	(0.16)	(0.10)	(0.19)	(0.11)	(0.18)	(0.16)	(0.21)	(0.10)	(0.11)	(0.16)	(0.12)	(0.10)	(0.28)
DoS attack (t-1)	2.06***	2.04***	2.06***	2.07***	2.06***	2.06***	2.03***	2.07***	2.07***	2.01***	2.04***	2.06***	2.07***	2.02***	2.06***	2.05***	2.02**	2.01***	2.05***	2.03***	2.01***	2.06***
	(0.37)	(0.36)	(0.36)	(0.36)	(0.36)	(0.36)	(0.36)	(0.36)	(0.35)	(0.33)	(0.36)	(0.36)	(0.36)	(0.39)	(0.35)	(0.37)	(0.36)	(0.37)	(0.37)	(0.37)	(0.36)	(0.37)
AIC	412.19	410.05	412.20	412.15	411.88	412.10	411.97	412.44	411.21	410.45	409.92	412.48	411.33	410.20	411.59	412.38	409.85	410.60	412.37	411.50	409.88	412.51
BIC	542.48	540.34	542.49	542.44	542.17	542.38	542.26	542.73	541.49	540.74	540.21	542.77	541.61	540.49	541.87	542.67	540.14	540.89	542.66	541.79	540.17	542.79
Log Likelihood	-185.10	-184.02	-185.10	-185.08	-184.94	-185.05	-184.98	-185.22	-184.60	-184.23	-183.96	-185.24	-184.66	-184.10	-184.79	-185.19	-183.92	-184.30	-185.19	-184.75	-183.94	-185.25
Deviance	370.19	368.05	370.20	370.15	369.88	370.10	369.97	370.44	369.21	368.45	367.92	370.48	369.33	368.20	369.59	370.38	367.85	368.60	370.37	369.50	367.88	370.51
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.03	0.10	−0.04	0.29	0.13	−0.30	0.04	−0.10	0.06	0.29	−0.16	−0.11**	−0.27*	0.22	−0.06	0.08	−0.17	−0.50*	−0.27	−0.02	−0.32	
	(0.14)	(0.18)	(0.13)	(0.22)	(0.20)	(0.26)	(0.21)	(0.08)	(0.13)	(0.21)	(0.09)	(0.04)	(0.13)	(0.19)	(0.13)	(0.12)	(0.12)	(0.21)	(0.19)	(0.26)	(0.23)	
DoS attack (t-1)	2.06***	2.05***	2.06***	2.08***	2.07***	2.02***	2.06***	2.05***	2.06***	2.04***	2.06***	2.05***	2.06***	2.04***	2.07***	2.06***	2.05***	2.06***	2.03***	2.06***	2.03***	
	(0.36)	(0.38)	(0.36)	(0.35)	(0.37)	(0.40)	(0.36)	(0.36)	(0.36)	(0.36)	(0.35)	(0.36)	(0.36)	(0.37)	(0.36)	(0.36)	(0.35)	(0.35)	(0.39)	(0.36)	(0.34)	
AIC	412.49	412.02	412.38	410.75	412.07	411.60	412.41	412.24	412.42	410.75	411.62	412.21	411.79	411.28	412.39	412.41	411.87	410.59	411.45	412.49	409.65	
BIC	542.78	542.30	542.67	541.04	542.35	541.28	542.69	542.53	542.70	541.04	541.91	542.50	542.07	541.57	542.68	542.70	542.16	540.88	541.73	542.77	539.93	
Log Likelihood	-185.24	-185.01	-185.19	-184.37	-185.03	-184.50	-185.20	-185.12	-185.21	-184.38	-184.81	-185.11	-184.89	-184.64	-185.20	-185.20	-184.94	-184.30	-184.72	-185.24	-183.82	
Deviance	370.49	370.02	370.38	368.75	370.07	369.00	370.41	370.24	370.42	368.75	369.62	370.21	369.79	369.28	370.39	370.41	369.87	368.59	369.45	370.49	367.65	
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	

Table D.4.26: Penalized logistic regression results (maximum proportion) - medium-term models (newspaper fixed effects). Note: Newspaper fixed are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.29	0.33*	−0.22	−0.02	−0.17	−0.18**	0.00	0.29**	−0.91***	0.25*	0.15	0.00	0.11	−0.18	0.26	0.38	0.33**	−0.21	0.22*	−0.18	−0.62***	−0.05
	(0.22)	(0.15)	(0.18)	(0.15)	(0.15)	(0.06)	(0.17)	(0.09)	(0.15)	(0.11)	(0.13)	(0.19)	(0.11)	(0.14)	(0.14)	(0.23)	(0.11)	(0.13)	(0.11)	(0.16)	(0.12)	(0.19)
DoS attack (t-1)	1.53***	1.51***	1.53***	1.53***	1.54***	1.54***	1.53***	1.53***	1.52***	1.52***	1.54***	1.53***	1.54***	1.53***	1.52***	1.49***	1.50***	1.51***	1.50***	1.50***	1.44***	1.53***
	(0.35)	(0.32)	(0.31)	(0.34)	(0.32)	(0.33)	(0.33)	(0.32)	(0.31)	(0.30)	(0.32)	(0.32)	(0.33)	(0.33)	(0.31)	(0.33)	(0.31)	(0.33)	(0.33)	(0.32)	(0.30)	(0.33)
AIC	437.07	435.81	436.59	437.50	437.10	436.93	437.53	436.07	435.76	436.99	437.24	437.58	437.14	437.06	436.41	436.15	434.80	436.60	436.59	436.68	431.47	437.55
BIC	710.05	708.80	709.58	710.48	710.08	709.91	710.51	709.05	708.74	709.97	710.22	710.56	710.12	710.04	709.39	709.13	707.78	709.58	709.57	709.67	704.45	710.53
Log Likelihood	-174.53	-173.91	-174.30	-174.75	-174.55	-174.46	-174.77	-174.03	-173.88	-174.50	-174.62	-174.79	-174.57	-174.53	-174.21	-174.08	-173.40	-174.30	-174.30	-174.34	-171.74	-174.77
Deviance	349.07	347.81	348.59	349.50	349.10	348.93	349.53	348.07	347.76	348.99	349.24	349.58	349.14	349.06	348.41	348.15	346.80	348.60	348.59	348.68	343.47	349.55
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.09	0.25	−0.12	0.29	0.02	−0.18	0.02	−0.10	0.14	0.30	−0.21*	0.09	−0.37**	0.22	−0.08	0.16	−0.34*	−1.01***	−0.19	−0.27	−0.24
	(0.10)	(0.17)	(0.15)	(0.15)	(0.20)	(0.21)	(0.16)	(0.09)	(0.13)	(0.20)	(0.09)	(0.14)	(0.13)	(0.24)	(0.19)	(0.14)	(0.14)	(0.16)	(0.17)	(0.23)	(0.24)
DoS attack (t-1)	1.53***	1.49***	1.52***	1.56***	1.54***	1.54***	1.54***	1.53***	1.54***	1.53***	1.53***	1.54***	1.53***	1.52***	1.54***	1.53***	1.50***	1.49***	1.52***	1.50***	1.53***
	(0.32)	(0.38)	(0.33)	(0.31)	(0.35)	(0.33)	(0.32)	(0.32)	(0.32)	(0.31)	(0.31)	(0.33)	(0.32)	(0.35)	(0.31)	(0.32)	(0.31)	(0.31)	(0.32)	(0.33)	(0.31)
AIC	437.46	434.86	436.95	436.27	437.40	437.17	437.41	437.35	437.27	435.93	436.19	437.49	436.13	436.61	437.38	437.16	435.67	431.22	437.05	436.25	435.99
BIC	710.44	707.84	709.94	709.25	710.39	710.16	710.40	710.34	710.25	708.91	709.17	710.48	709.12	709.60	710.37	710.14	708.65	704.20	710.03	709.23	708.97
Log Likelihood	-174.73	-173.43	-174.48	-174.13	-174.70	-174.59	-174.71	-174.68	-174.63	-173.97	-174.09	-174.75	-174.07	-174.31	-174.69	-174.58	-173.84	-171.61	-174.52	-174.12	-174.00
Deviance	349.46	346.86	348.95	348.27	349.40	349.17	349.41	349.35	349.27	347.93	348.19	349.49	348.13	348.61	349.38	349.16	347.67	343.22	349.05	348.25	347.99
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.27: Penalized logistic regression results (maximum proportion) - medium-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.25	0.45***	−0.15	0.05	0.00	−0.17	0.18	0.49***	−0.46***	0.22	0.34*	0.12	−0.01	−0.37*	0.11	0.42*	0.18	−0.69	0.38***	0.02	−0.75***	−0.15
	(0.17)	(0.11)	(0.16)	(0.16)	(0.11)	(0.15)	(0.13)	(0.07)	(0.10)	(0.12)	(0.15)	(0.16)	(0.09)	(0.15)	(0.11)	(0.17)	(0.14)	(0.18)	(0.08)	(0.16)	(0.11)	(0.13)
DoS attack (t-1)	2.92***	2.95***	2.90***	2.93***	2.94***	2.90***	2.91***	2.87***	2.89***	2.89***	2.95***	2.94***	2.94***	3.04***	2.90***	2.87***	2.85***	2.91***	2.95***	2.94***	2.88***	2.93***
	(0.42)	(0.36)	(0.39)	(0.38)	(0.40)	(0.39)	(0.40)	(0.38)	(0.37)	(0.37)	(0.37)	(0.38)	(0.37)	(0.38)	(0.35)	(0.41)	(0.40)	(0.40)	(0.39)	(0.39)	(0.32)	(0.41)
AIC	353.35	350.99	353.09	353.52	353.64	353.07	353.09	350.28	353.26	353.22	352.29	353.50	353.43	351.52	353.48	351.74	352.84	353.37	351.08	353.51	346.35	353.31
BIC	750.42	748.05	750.15	750.59	750.70	750.13	750.16	747.34	750.32	750.28	749.35	750.57	750.50	748.58	750.54	748.80	749.90	750.44	748.15	750.58	743.41	750.38
Log Likelihood	-112.68	-111.49	-112.55	-112.76	-112.82	-112.53	-112.55	-111.14	-112.63	-112.61	-112.14	-112.75	-112.72	-111.76	-112.74	-111.87	-112.42	-112.69	-111.54	-112.76	-109.18	-112.66
Deviance	225.35	222.99	225.09	225.52	225.64	225.07	225.09	222.28	225.26	225.22	224.29	225.50	225.43	223.52	225.48	223.74	224.84	225.37	223.08	225.51	218.35	225.31
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.14	0.19	−0.00	0.35***	0.08	−0.31	0.27	−0.24*	0.15	0.60***	−0.13	0.10	−0.15	0.25	0.13	0.21	−0.43***	−1.10***	−0.13	−0.23	−0.31
	(0.15)	(0.13)	(0.11)	(0.10)	(0.15)	(0.24)	(0.16)	(0.11)	(0.12)	(0.14)	(0.08)	(0.15)	(0.08)	(0.21)	(0.17)	(0.12)	(0.10)	(0.15)	(0.11)	(0.17)	(0.16)
DoS attack (t-1)	2.93***	2.90***	2.93***	2.90***	2.94***	2.95***	3.03***	2.95***	2.93***	3.03***	2.92***	2.93***	2.94***	3.01***	2.94***	2.90***	2.83***	2.79***	2.91***	2.90***	2.92***
	(0.38)	(0.44)	(0.38)	(0.35)	(0.38)	(0.42)	(0.39)	(0.39)	(0.38)	(0.32)	(0.37)	(0.39)	(0.38)	(0.39)	(0.39)	(0.38)	(0.36)	(0.39)	(0.39)	(0.41)	(0.37)
AIC	353.43	352.14	353.46	351.89	353.35	352.51	352.12	352.59	353.38	347.52	352.95	353.50	353.36	352.46	353.29	353.03	351.02	346.83	353.46	352.76	350.92	
BIC	750.50	749.20	750.52	748.96	750.42	749.58	749.18	749.66	750.44	744.59	750.01	750.56	750.43	749.53	750.35	750.09	748.08	743.90	750.53	749.83	747.98	
Log Likelihood	-112.72	-112.07	-112.73	-111.95	-112.68	-112.26	-112.06	-112.30	-112.69	-109.76	-112.47	-112.75	-112.68	-112.23	-112.64	-112.51	-111.51	-109.42	-112.73	-112.38	-111.46	
Deviance	225.43	224.14	225.46	223.89	225.35	224.51	224.12	224.59	225.38	219.52	224.95	225.50	225.36	224.46	225.29	225.03	223.02	218.83	225.46	224.76	222.92	
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	

Table D.4.28: Penalized logistic regression results (maximum proportion) - medium-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	LeBlat opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	−0.29*	0.20***	−0.06	0.15	−0.03	0.04	0.11	0.15	−0.26	−0.12	0.01	−0.28*	0.17	−0.32	0.01	0.14	0.02	0.08	−0.38*	−0.18	0.02	0.02	0.05
	(0.14)	(0.06)	(0.12)	(0.09)	(0.09)	(0.10)	(0.11)	(0.09)	(0.18)	(0.14)	(0.18)	(0.11)	(0.17)	(0.30)	(0.17)	(0.11)	(0.17)	(0.13)	(0.18)	(0.30)	(0.11)	(0.07)	(0.08)
Number of headlines	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.01	0.00	0.00	0.00	−0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.41***	2.36***	2.46***	2.43***	2.45***	2.45***	2.42***	2.43***	2.45***	2.45***	2.45***	2.42***	2.42***	2.42***	2.45***	2.43***	2.46***	2.44***	2.41***	2.42***	2.45***	2.45***	2.45***
	(0.30)	(0.33)	(0.29)	(0.28)	(0.29)	(0.29)	(0.30)	(0.31)	(0.31)	(0.30)	(0.29)	(0.29)	(0.29)	(0.28)	(0.29)	(0.30)	(0.31)	(0.30)	(0.29)	(0.32)	(0.29)	(0.29)	(0.30)
AIC	1017.33	1016.45	1023.65	1020.47	1021.97	1024.09	1022.59	1020.20	1019.21	1022.60	1024.16	1019.00	1020.33	1017.89	1024.18	1022.05	1024.15	1023.54	1017.37	1021.52	1024.12	1024.17	1023.53
BIC	1042.03	1041.15	1048.34	1045.16	1048.67	1048.78	1047.29	1044.90	1043.91	1047.29	1048.86	1043.70	1045.03	1042.59	1048.87	1046.74	1048.85	1048.23	1042.06	1046.21	1048.82	1048.87	1048.63
Log Likelihood	-504.67	-504.23	-507.82	-506.23	-507.99	-508.04	-507.30	-506.10	-505.61	-507.30	-508.08	-505.50	-506.17	-504.95	-508.09	-507.02	-508.08	-507.77	-504.68	-506.76	-508.06	-508.08	-507.97
Deviance	1009.33	1008.45	1015.65	1012.47	1015.97	1016.09	1014.59	1012.20	1011.21	1014.60	1016.16	1011.00	1012.33	1009.89	1016.18	1014.05	1016.15	1015.54	1009.37	1013.52	1016.12	1016.17	1015.93
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.07	0.12	0.04	0.20	0.16	−0.31*	0.06	0.14***	−0.17	0.03	−0.16	−0.25	−0.01	−0.06	0.16	−0.06	−0.07	−0.16	0.14	0.12	−0.29**	−0.00	0.10
	(0.12)	(0.13)	(0.10)	(0.16)	(0.12)	(0.16)	(0.13)	(0.04)	(0.15)	(0.10)	(0.20)	(0.16)	(0.11)	(0.15)	(0.10)	(0.20)	(0.14)	(0.12)	(0.12)	(0.10)	(0.23)	(0.08)	(0.08)
Number of headlines	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.45***	2.42***	2.46***	2.42***	2.44***	2.44***	2.45***	2.40***	2.43***	2.46***	2.44***	2.43***	2.45***	2.46***	2.44***	2.45***	2.45***	2.45***	2.44***	2.44***	2.39***	2.46***	2.44***
	(0.29)	(0.29)	(0.29)	(0.32)	(0.31)	(0.30)	(0.29)	(0.31)	(0.31)	(0.29)	(0.30)	(0.29)	(0.29)	(0.29)	(0.30)	(0.30)	(0.29)	(0.30)	(0.29)	(0.29)	(0.29)	(0.29)	(0.31)
AIC	1023.77	1022.36	1024.12	1017.60	1020.25	1018.90	1023.80	1019.40	1021.17	1024.14	1021.59	1019.71	1024.14	1023.70	1020.85	1023.72	1023.54	1022.91	1021.71	1022.26	1024.84	1024.15	1022.56
BIC	1048.47	1047.06	1048.82	1042.29	1044.95	1043.60	1048.50	1044.10	1045.87	1048.83	1046.29	1044.40	1048.83	1048.40	1045.54	1048.41	1048.23	1047.61	1046.41	1046.95	1037.53	1048.84	1047.26
Log Likelihood	-507.89	-507.18	-508.06	-504.80	-506.13	-505.45	-507.90	-505.70	-506.59	-508.07	-506.80	-505.85	-508.07	-507.85	-506.42	-507.86	-507.77	-507.46	-506.86	-507.13	-502.42	-508.07	-507.28
Deviance	1015.77	1014.36	1016.12	1009.60	1012.25	1010.90	1015.80	1011.40	1013.17	1016.14	1013.59	1011.71	1016.14	1015.70	1012.85	1015.72	1015.54	1014.91	1013.73	1014.26	1004.84	1016.15	1014.56
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.29: Penalized logistic regression results (5XX error codes) - short-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.22	0.02	−0.19**	0.15**	−0.02	0.09	0.03	0.02	−0.30*	−0.07	−0.04	−0.20	0.07	−0.09	0.09	0.03	−0.13	0.05	0.01	0.04	0.04
	(0.20)	(0.04)	(0.07)	(0.06)	(0.08)	(0.10)	(0.04)	(0.07)	(0.15)	(0.08)	(0.07)	(0.18)	(0.07)	(0.05)	(0.10)	(0.10)	(0.24)	(0.10)	(0.04)	(0.06)	(0.10)
DoS attack (t-1)	1.41***	1.42***	1.41***	1.41***	1.42***	1.42***	1.42***	1.42***	1.41***	1.43***	1.43***	1.37***	1.42***	1.41***	1.44***	1.42***	1.40***	1.42***	1.42***	1.42***	1.42***
	(0.27)	(0.25)	(0.25)	(0.24)	(0.25)	(0.25)	(0.25)	(0.25)	(0.26)	(0.25)	(0.25)	(0.30)	(0.25)	(0.26)	(0.26)	(0.26)	(0.28)	(0.26)	(0.25)	(0.26)	(0.25)
AIC	910.05	911.31	908.32	907.89	911.34	910.85	911.24	911.33	909.61	910.93	911.12	906.21	910.89	910.28	910.99	911.35	910.41	911.14	911.39	911.21	911.37
BIC	1039.70	1040.97	1037.97	1037.54	1040.99	1040.50	1040.89	1040.98	1039.26	1040.58	1040.77	1035.86	1040.54	1039.93	1040.64	1041.00	1040.06	1040.79	1041.04	1040.86	1041.02
Log Likelihood	-434.02	-434.66	-433.16	-432.95	-434.67	-434.43	-434.62	-434.66	-433.80	-434.46	-434.56	-432.10	-434.45	-434.14	-434.49	-434.67	-434.20	-434.57	-434.69	-434.60	-434.68
Deviance	868.05	869.31	866.32	865.89	869.34	868.85	869.24	869.33	867.61	868.93	869.12	864.21	868.89	868.28	868.99	869.35	868.41	869.14	869.39	869.21	869.37
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.05	0.01	0.37***	0.13***	−0.00	0.07	0.10**	−0.11	−0.08	−0.09	−0.07	−0.10*	−0.07	0.18	−0.11	0.16	0.00	0.08	0.01	0.07	0.03
	(0.12)	(0.04)	(0.07)	(0.03)	(0.15)	(0.14)	(0.03)	(0.08)	(0.09)	(0.13)	(0.11)	(0.04)	(0.12)	(0.10)	(0.18)	(0.13)	(0.05)	(0.08)	(0.07)	(0.07)	(0.04)
DoS attack (t-1)	1.41***	1.42***	1.34***	1.42***	1.42***	1.42***	1.40***	1.41***	1.40***	1.42***	1.42***	1.40***	1.43***	1.41***	1.41***	1.41***	1.42***	1.42***	1.42***	1.41***	1.42***
	(0.27)	(0.25)	(0.31)	(0.26)	(0.25)	(0.25)	(0.27)	(0.25)	(0.28)	(0.25)	(0.25)	(0.26)	(0.25)	(0.26)	(0.26)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)
AIC	911.18	911.38	899.06	908.75	911.61	911.14	909.22	910.27	910.51	910.79	911.17	909.96	910.97	908.71	910.55	910.39	911.39	910.86	911.38	910.99	911.28
BIC	1040.83	1041.04	1028.71	1038.40	1041.26	1040.79	1038.87	1039.92	1040.16	1040.44	1040.82	1039.61	1040.63	1038.36	1040.20	1040.04	1041.04	1040.51	1041.03	1040.64	1040.93
Log Likelihood	-434.59	-434.69	-428.53	-433.37	-434.80	-434.57	-433.61	-434.14	-434.25	-434.39	-434.59	-433.98	-434.49	-433.36	-434.27	-434.20	-434.70	-434.43	-434.69	-434.49	-434.64
Deviance	869.18	869.38	857.06	866.75	869.61	869.14	867.22	868.27	868.51	868.79	869.17	867.96	868.97	866.71	868.55	868.39	869.39	868.86	869.38	868.99	869.28
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.30: Penalized logistic regression results (5XX error codes) - short-term models (newspaper fixed effects). Note: Newspaper fixed are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.27	0.06*	−0.24*	0.18***	−0.04	0.08	0.07	0.13**	−0.30*	−0.10	−0.18**	−0.37*	0.08	−0.12**	0.07	0.02	−0.06	0.06	0.01	0.06	−0.01
	(0.21)	(0.03)	(0.11)	(0.04)	(0.08)	(0.09)	(0.04)	(0.05)	(0.13)	(0.09)	(0.07)	(0.19)	(0.05)	(0.04)	(0.11)	(0.06)	(0.22)	(0.10)	(0.04)	(0.05)	(0.09)
DoS attack (t-1)	1.22***	1.23***	1.22***	1.21***	1.23***	1.23***	1.23***	1.23***	1.21***	1.23***	1.24***	1.17***	1.23***	1.21***	1.24***	1.23***	1.22***	1.23***	1.23***	1.22***	1.23***
	(0.27)	(0.26)	(0.25)	(0.26)	(0.25)	(0.26)	(0.26)	(0.25)	(0.26)	(0.25)	(0.26)	(0.30)	(0.26)	(0.26)	(0.27)	(0.26)	(0.26)	(0.26)	(0.25)	(0.27)	(0.26)
AIC	944.39	945.70	941.78	942.19	946.15	945.92	945.62	943.81	944.30	945.46	943.42	938.86	945.73	944.86	946.01	946.23	946.06	945.97	946.24	945.91	946.25
BIC	1246.91	1248.22	1244.30	1244.71	1248.67	1248.44	1248.14	1246.33	1246.82	1247.98	1245.93	1241.38	1248.24	1247.38	1248.53	1248.75	1248.58	1248.49	1248.76	1248.43	1248.77
Log Likelihood	-423.19	-423.85	-421.89	-422.09	-424.07	-423.96	-423.81	-422.90	-423.15	-423.73	-422.71	-420.43	-423.86	-423.43	-424.00	-424.11	-424.03	-423.99	-424.12	-423.96	-424.12
Deviance	846.39	847.70	843.78	844.19	848.15	847.92	847.62	845.81	846.30	847.46	845.42	840.86	847.73	846.86	848.01	848.23	848.06	847.97	848.24	847.91	848.25
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.08	0.02	0.40***	0.09*	0.00	0.09	0.09***	−0.09	−0.10	−0.09	−0.04	−0.08	−0.09	0.19***	−0.11	0.15	−0.02	0.07	0.03	0.03	0.09*
	(0.06)	(0.05)	(0.06)	(0.04)	(0.15)	(0.13)	(0.03)	(0.09)	(0.09)	(0.16)	(0.18)	(0.05)	(0.14)	(0.06)	(0.18)	(0.14)	(0.06)	(0.09)	(0.05)	(0.07)	(0.05)
DoS attack (t-1)	1.22***	1.23***	1.15***	1.24***	1.23***	1.23***	1.21***	1.23***	1.21***	1.23***	1.23***	1.21***	1.24***	1.23***	1.22***	1.23***	1.23***	1.23***	1.23***	1.22***	1.22***
	(0.26)	(0.25)	(0.28)	(0.25)	(0.26)	(0.25)	(0.26)	(0.26)	(0.28)	(0.25)	(0.25)	(0.27)	(0.25)	(0.27)	(0.26)	(0.25)	(0.25)	(0.26)	(0.25)	(0.26)	(0.26)
AIC	945.86	946.24	933.90	945.08	946.52	945.80	944.45	945.68	945.23	945.76	946.29	945.45	945.55	943.35	945.56	945.54	946.24	945.84	946.18	946.20	945.14
BIC	1248.38	1248.76	1236.41	1247.60	1249.04	1248.32	1246.97	1248.20	1247.75	1248.28	1248.81	1247.97	1248.07	1245.87	1248.08	1248.06	1248.76	1248.36	1248.70	1248.71	1247.66
Log Likelihood	-423.93	-424.12	-417.95	-423.54	-424.26	-423.90	-423.23	-423.84	-423.62	-423.88	-424.14	-423.72	-423.77	-422.67	-423.78	-423.77	-424.12	-423.92	-424.09	-424.10	-423.57
Deviance	847.86	848.24	835.90	847.08	848.52	847.80	846.45	847.68	847.23	847.76	848.29	847.45	847.55	845.35	847.56	847.54	848.24	847.84	848.18	848.20	847.14
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.31: Penalized logistic regression results (5XX error codes) - short-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.29	0.08*	−0.23	0.24***	−0.03	0.10	0.00	0.11	−0.44***	−0.13*	−0.31***	−0.42*	0.14**	−0.15**	0.05	−0.03	−0.06	0.08	−0.00	0.21**	−0.03
	(0.22)	(0.04)	(0.13)	(0.06)	(0.11)	(0.08)	(0.05)	(0.06)	(0.12)	(0.05)	(0.05)	(0.18)	(0.05)	(0.05)	(0.07)	(0.07)	(0.18)	(0.11)	(0.07)	(0.07)	(0.08)
DoS attack (t-1)	1.76***	1.81***	1.75***	1.79***	1.79***	1.82***	1.79***	1.79***	1.79***	1.79***	1.79***	1.74***	1.80***	1.78***	1.80***	1.79**	1.78***	1.79***	1.79***	1.78***	1.79***
	(0.19)	(0.18)	(0.19)	(0.19)	(0.18)	(0.18)	(0.19)	(0.18)	(0.21)	(0.19)	(0.18)	(0.21)	(0.19)	(0.19)	(0.19)	(0.18)	(0.19)	(0.18)	(0.18)	(0.20)	(0.19)
AIC	925.00	926.37	923.73	921.89	927.24	926.61	927.20	925.64	923.21	926.31	921.21	917.95	925.36	925.00	927.18	927.09	927.11	926.87	927.25	923.80	927.17
BIC	1715.26	1716.62	1713.99	1712.14	1717.49	1716.86	1717.46	1715.89	1713.46	1716.57	1711.46	1708.21	1715.62	1715.25	1717.43	1717.35	1717.36	1717.13	1717.51	1714.05	1717.43
Log Likelihood	-334.50	-335.18	-333.87	-332.95	-335.62	-335.31	-335.60	-334.82	-333.60	-335.16	-332.60	-330.98	-334.68	-334.50	-335.59	-335.55	-335.55	-335.44	-335.63	-333.90	-335.59
Deviance	669.00	670.37	667.73	665.89	671.24	670.61	671.20	669.64	667.21	670.31	665.21	661.95	669.36	669.00	671.18	671.09	671.11	670.87	671.25	667.80	671.17
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.00	0.01	0.40***	0.13***	−0.22	0.22	0.16**	0.07	−0.12	−0.23	−0.12	0.01	−0.03	0.33***	−0.20	0.23	−0.11	0.09	−0.02	0.12	0.20***
	(0.07)	(0.06)	(0.07)	(0.04)	(0.16)	(0.12)	(0.05)	(0.10)	(0.08)	(0.14)	(0.13)	(0.05)	(0.13)	(0.08)	(0.18)	(0.14)	(0.07)	(0.09)	(0.05)	(0.08)	(0.06)
DoS attack (t-1)	1.79***	1.79***	1.76***	1.79***	1.82***	1.76***	1.74***	1.79***	1.76***	1.80***	1.79***	1.79***	1.79***	1.77***	1.80***	1.77***	1.80***	1.80***	1.79***	1.77***	1.81***
	(0.19)	(0.18)	(0.19)	(0.19)	(0.19)	(0.17)	(0.20)	(0.19)	(0.19)	(0.18)	(0.18)	(0.19)	(0.18)	(0.19)	(0.18)	(0.18)	(0.19)	(0.19)	(0.19)	(0.19)	(0.20)
AIC	927.28	927.19	916.91	925.00	926.66	924.39	923.00	927.07	925.89	924.51	926.96	927.22	927.29	920.11	925.40	925.56	926.61	926.86	927.14	926.37	922.49
BIC	1717.53	1717.44	1707.16	1715.25	1716.91	1714.64	1713.25	1717.33	1716.14	1714.76	1717.22	1717.47	1717.54	1710.37	1715.65	1715.82	1716.87	1717.12	1717.39	1716.62	1712.74
Log Likelihood	-335.64	-335.60	-330.46	-334.50	-335.33	-334.19	-333.50	-335.54	-334.94	-334.25	-335.48	-335.61	-335.64	-332.06	-334.79	-334.78	-335.31	-335.43	-335.57	-335.18	-333.24
Deviance	671.28	671.19	660.91	669.00	670.66	668.39	667.00	671.07	669.89	668.51	670.96	671.22	671.29	664.11	669.40	669.56	670.61	670.86	671.14	670.37	666.49
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.32: Penalized logistic regression results (5XX error codes) - short-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	−0.33	0.18**	0.05	0.13	−0.01	−0.08	0.07	0.24***	−0.24	−0.14	0.12	−0.32	0.21	−3.58**	0.07	0.16	−0.14	0.17	−0.40*	−0.22	0.06	0.04	0.09
	(0.20)	(0.07)	(0.09)	(0.10)	(0.13)	(0.11)	(0.16)	(0.07)	(0.23)	(0.24)	(0.23)	(0.22)	(0.19)	(1.28)	(0.19)	(0.12)	(0.22)	(0.18)	(0.19)	(0.24)	(0.23)	(0.08)	(0.10)
Number of headlines	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.01	0.00	0.01	0.00	−0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.39***	2.40***	2.45***	2.42***	2.45***	2.45***	2.45***	2.33***	2.42***	2.44***	2.44***	2.40***	2.39***	2.23***	2.45***	2.43***	2.44***	2.43***	2.41***	2.41***	2.45***	2.45***	2.44***
	(0.30)	(0.31)	(0.30)	(0.28)	(0.30)	(0.29)	(0.30)	(0.33)	(0.31)	(0.31)	(0.29)	(0.28)	(0.31)	(0.29)	(0.30)	(0.31)	(0.32)	(0.32)	(0.30)	(0.31)	(0.29)	(0.29)	(0.29)
AIC	1015.78	1018.82	1023.88	1021.64	1024.03	1022.27	1023.64	1012.59	1019.57	1021.69	1022.00	1016.97	1017.37	991.33	1023.67	1021.17	1021.98	1020.02	1016.95	1019.59	1023.64	1023.96	1022.58
BIC	1040.47	1043.51	1048.58	1046.33	1048.72	1047.96	1048.34	1037.28	1044.26	1046.39	1046.69	1041.67	1042.06	1016.02	1048.37	1045.87	1046.67	1044.72	1041.64	1044.28	1048.33	1048.66	1047.68
Log Likelihood	-503.89	-505.41	-507.94	-506.82	-508.01	-507.63	-507.82	-502.29	-505.78	-506.85	-507.00	-504.49	-504.68	-491.66	-507.84	-506.59	-506.99	-506.01	-504.47	-505.79	-507.82	-507.98	-507.49
Deviance	1007.78	1010.82	1015.88	1013.64	1016.03	1015.27	1015.64	1004.59	1011.57	1013.69	1014.00	1008.97	1009.37	983.33	1015.67	1013.17	1013.98	1012.02	1008.95	1011.59	1015.64	1015.96	1014.98
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.01	0.10	−0.09	0.02	0.19	−0.32	0.10	0.14*	−0.14	−0.01	−0.09	−0.24	−0.04	−0.12	0.13	−0.03	−0.20	−0.11	0.21	0.26*	−0.57***	0.02	0.02
	(0.14)	(0.17)	(0.13)	(0.18)	(0.17)	(0.22)	(0.14)	(0.06)	(0.22)	(0.11)	(0.19)	(0.16)	(0.11)	(0.19)	(0.09)	(0.20)	(0.16)	(0.12)	(0.14)	(0.12)	(0.16)	(0.11)	(0.13)
Number of headlines	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.01	0.00	0.01	0.01	0.00	0.00	0.00
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.45***	2.44***	2.45***	2.45***	2.39***	2.42**	2.44***	2.40***	2.44***	2.45***	2.44***	2.42***	2.45***	2.44***	2.43***	2.45***	2.42***	2.44***	2.42***	2.35***	2.49***	2.45***	2.45***
	(0.29)	(0.29)	(0.29)	(0.29)	(0.35)	(0.31)	(0.28)	(0.31)	(0.31)	(0.29)	(0.30)	(0.28)	(0.29)	(0.30)	(0.29)	(0.30)	(0.29)	(0.30)	(0.29)	(0.35)	(0.29)	(0.29)	(0.30)
AIC	1024.06	1022.81	1022.97	1024.07	1017.54	1018.77	1022.80	1020.37	1022.02	1024.04	1023.09	1020.30	1023.82	1022.55	1021.97	1023.88	1020.61	1022.65	1018.09	1012.59	1014.32	1024.06	1024.08
BIC	1048.75	1047.50	1047.66	1048.77	1042.24	1043.46	1047.49	1045.06	1046.71	1048.73	1047.78	1044.99	1048.51	1047.25	1046.66	1048.57	1045.31	1047.35	1042.78	1037.20	1039.01	1048.76	1048.77
Log Likelihood	-508.03	-507.41	-507.48	-508.04	-504.77	-505.39	-507.40	-506.18	-507.01	-508.02	-507.54	-506.15	-507.91	-507.28	-506.98	-507.94	-506.31	-507.33	-505.05	-502.25	-503.16	-508.03	-508.04
Deviance	1016.06	1014.81	1014.97	1016.07	1009.54	1010.77	1014.80	1012.37	1014.02	1016.04	1015.09	1012.30	1015.82	1014.55	1013.97	1015.88	1012.61	1014.65	1010.09	1004.50	1006.32	1016.06	1016.08
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.4.33: Penalized logistic regression results (5XX error codes) - medium-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.43*	−0.20***	−0.09	0.11	0.01	−0.17**	−0.05	0.05	−0.21	−0.03	0.06	−0.45***	0.11	−0.06	−0.22	0.10	−0.07	0.12	0.04	0.13	−0.14
	(0.21)	(0.04)	(0.08)	(0.09)	(0.08)	(0.06)	(0.04)	(0.04)	(0.33)	(0.08)	(0.08)	(0.08)	(0.06)	(0.07)	(0.19)	(0.15)	(0.19)	(0.09)	(0.05)	(0.07)	(0.14)
DoS attack (t-1)	1.61***	1.60***	1.64***	1.63***	1.65***	1.65***	1.64***	1.64***	1.64***	1.65***	1.64***	1.57***	1.64***	1.64***	1.63***	1.63***	1.65***	1.64***	1.64***	1.62***	1.64***
	(0.34)	(0.35)	(0.32)	(0.30)	(0.31)	(0.31)	(0.31)	(0.31)	(0.32)	(0.31)	(0.31)	(0.37)	(0.31)	(0.32)	(0.33)	(0.34)	(0.32)	(0.31)	(0.31)	(0.33)	(0.31)
AIC	973.14	970.71	975.29	974.16	975.93	974.51	975.46	975.48	975.62	975.80	975.66	966.90	974.75	975.40	974.00	975.07	975.39	974.76	975.72	973.39	974.86
BIC	1103.43	1101.00	1105.58	1104.45	1106.22	1104.80	1105.74	1105.76	1105.91	1106.08	1105.95	1097.19	1105.03	1105.69	1104.29	1105.36	1105.68	1105.05	1106.01	1103.68	1105.15
Log Likelihood	-465.57	-464.36	-466.65	-466.08	-466.97	-466.25	-466.73	-466.74	-466.81	-466.90	-466.83	-462.45	-466.37	-466.70	-466.00	-466.53	-466.69	-466.38	-466.86	-465.70	-466.43
Deviance	931.14	928.71	933.29	932.16	933.93	932.51	933.46	933.48	933.62	933.80	933.66	924.90	932.75	933.40	932.00	933.07	933.39	932.76	933.72	931.39	932.86
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.03	−0.06	0.02	0.19**	0.11	0.26	0.06	−0.01	−0.13	0.16	−0.08	−0.19***	−0.23*	0.16	−0.13	0.16	0.06	0.15	0.19	0.30*	−0.04
	(0.19)	(0.04)	(0.12)	(0.06)	(0.20)	(0.16)	(0.03)	(0.11)	(0.10)	(0.12)	(0.10)	(0.04)	(0.09)	(0.08)	(0.13)	(0.18)	(0.06)	(0.10)	(0.11)	(0.14)	(0.03)
DoS attack (t-1)	1.65***	1.64***	1.64***	1.60***	1.65***	1.63***	1.63***	1.65***	1.63***	1.65***	1.64***	1.60***	1.63**	1.63***	1.63***	1.65***	1.64***	1.64***	1.60***	1.59***	1.64***
	(0.31)	(0.31)	(0.32)	(0.35)	(0.31)	(0.33)	(0.32)	(0.31)	(0.34)	(0.31)	(0.31)	(0.33)	(0.32)	(0.30)	(0.32)	(0.31)	(0.31)	(0.32)	(0.37)	(0.32)	(0.31)
AIC	975.80	975.24	975.86	971.39	976.23	972.61	975.23	975.89	974.14	974.63	975.82	970.63	973.43	973.67	974.97	975.29	975.58	974.58	971.75	970.61	975.38
BIC	1106.09	1105.53	1106.14	1101.67	1106.52	1102.89	1105.51	1106.18	1104.42	1104.91	1106.11	1100.92	1103.72	1103.96	1105.26	1105.58	1105.86	1104.87	1102.04	1100.90	1105.67
Log Likelihood	-466.90	-466.62	-466.93	-464.69	-467.11	-465.30	-466.61	-466.95	-466.07	-466.31	-466.91	-464.32	-465.72	-465.84	-466.49	-466.65	-466.79	-466.29	-464.88	-464.31	-466.69
Deviance	933.80	933.24	933.86	929.39	934.23	930.61	933.23	933.89	932.14	932.63	933.82	928.63	931.43	931.67	932.97	933.29	933.58	932.58	929.75	928.61	933.38
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.34: Penalized logistic regression results (5XX error codes) - medium-term models (newspaper fixed effects). Note: Newspaper effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.50*	−0.17***	−0.01	0.09	−0.01	−0.23	−0.06	0.17**	−0.33	−0.14	−0.20	−0.53***	0.24**	−0.04	−0.24	0.19	−0.03	0.15	0.12	0.15*	−0.30*
	(0.22)	(0.04)	(0.11)	(0.12)	(0.08)	(0.17)	(0.04)	(0.05)	(0.41)	(0.13)	(0.13)	(0.11)	(0.09)	(0.04)	(0.22)	(0.19)	(0.20)	(0.11)	(0.07)	(0.06)	(0.13)
DoS attack (t-1)	1.42***	1.42***	1.45***	1.43***	1.45***	1.46***	1.44***	1.42***	1.43***	1.44***	1.44***	1.34***	1.42***	1.44***	1.42***	1.43***	1.45***	1.44***	1.44***	1.42***	1.43***
	(0.34)	(0.34)	(0.32)	(0.33)	(0.32)	(0.31)	(0.32)	(0.32)	(0.34)	(0.32)	(0.30)	(0.38)	(0.33)	(0.32)	(0.35)	(0.35)	(0.32)	(0.32)	(0.32)	(0.33)	(0.31)
AIC	1007.78	1007.79	1010.89	1010.07	1010.87	1009.12	1010.31	1007.11	1009.99	1009.77	1008.87	998.40	1007.11	1010.62	1008.88	1009.00	1010.78	1009.65	1010.07	1008.63	1007.84
BIC	1311.78	1311.79	1314.89	1314.07	1314.87	1313.12	1314.31	1311.11	1313.99	1313.77	1312.88	1302.40	1311.11	1314.62	1312.88	1313.00	1314.79	1313.66	1314.08	1312.63	1311.84
Log Likelihood	-454.89	-454.89	-456.44	-456.03	-456.43	-455.56	-456.15	-454.55	-456.00	-455.88	-455.44	-450.20	-454.55	-456.31	-455.44	-455.50	-456.39	-455.83	-456.04	-455.31	-454.92
Deviance	909.78	909.79	912.89	912.07	912.87	911.12	912.31	909.11	911.99	911.77	910.87	900.40	909.11	912.62	910.88	911.00	912.78	911.65	912.07	910.63	909.84
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.08	0.00	−0.00	0.16*	0.09	0.49***	0.12**	−0.01	−0.18	0.26	−0.24*	−0.15	−0.32*	0.31***	−0.06	0.14	0.03	0.17	0.28***	0.39**	−0.02
	(0.16)	(0.05)	(0.07)	(0.08)	(0.19)	(0.11)	(0.04)	(0.13)	(0.09)	(0.15)	(0.12)	(0.08)	(0.14)	(0.09)	(0.13)	(0.19)	(0.07)	(0.10)	(0.08)	(0.15)	(0.04)
DoS attack (t-1)	1.45***	1.45***	1.45***	1.42***	1.45***	1.41***	1.42***	1.45***	1.42***	1.44***	1.44***	1.43***	1.42***	1.42***	1.45***	1.45***	1.45***	1.44***	1.40***	1.39***	1.45***
	(0.32)	(0.32)	(0.32)	(0.33)	(0.32)	(0.32)	(0.32)	(0.32)	(0.35)	(0.32)	(0.31)	(0.34)	(0.32)	(0.32)	(0.32)	(0.31)	(0.32)	(0.32)	(0.35)	(0.35)	(0.32)
AIC	1010.55	1010.84	1010.82	1008.37	1011.20	1002.24	1008.79	1010.86	1008.40	1008.77	1009.78	1008.66	1006.56	1007.13	1010.73	1010.48	1010.79	1009.68	1003.99	1005.43	1010.73
BIC	1314.55	1314.84	1314.83	1312.37	1315.21	1306.25	1312.80	1314.87	1312.40	1312.78	1313.78	1312.66	1310.56	1311.13	1314.73	1314.48	1314.80	1313.68	1307.99	1309.43	1314.73
Log Likelihood	-456.27	-456.42	-456.41	-455.18	-456.60	-452.12	-455.40	-456.43	-455.20	-455.39	-455.89	-455.33	-454.28	-454.56	-456.37	-456.24	-456.40	-455.84	-453.00	-453.71	-456.36
Deviance	912.55	912.84	912.82	910.37	913.20	904.24	910.79	912.86	910.40	910.77	911.78	910.66	908.56	909.13	912.73	912.48	912.79	911.68	905.99	907.43	912.73
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.35: Penalized logistic regression results (5XX error codes) - medium-term models (newspaper and week fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.70***	−0.14***	−0.06	0.11	0.02	−0.21	−0.09*	0.28***	−0.25	−0.17	−0.14	−0.57***	0.34**	−0.08	−0.27	0.21	−0.10	0.13	0.24***	0.21**	−0.31**
	(0.19)	(0.04)	(0.13)	(0.09)	(0.10)	(0.20)	(0.03)	(0.06)	(0.32)	(0.11)	(0.13)	(0.09)	(0.07)	(0.05)	(0.23)	(0.17)	(0.15)	(0.10)	(0.07)	(0.06)	(0.12)
DoS attack (t-1)	1.97***	1.94***	1.98***	1.97***	1.99***	1.97***	1.99***	1.97***	1.97***	1.97***	1.97***	1.89***	1.98***	1.99***	1.96***	1.97***	1.99***	1.97***	2.00***	1.93***	1.95***
	(0.24)	(0.23)	(0.21)	(0.22)	(0.22)	(0.20)	(0.22)	(0.22)	(0.23)	(0.21)	(0.20)	(0.26)	(0.23)	(0.21)	(0.23)	(0.23)	(0.21)	(0.22)	(0.21)	(0.24)	(0.21)
AIC	969.12	972.92	974.85	973.79	975.01	973.71	973.94	965.62	974.62	973.56	974.11	959.12	967.79	974.31	972.56	972.51	974.57	974.04	972.13	971.23	971.47
BIC	1763.25	1767.05	1768.98	1767.91	1769.14	1767.84	1768.07	1759.75	1768.74	1767.69	1768.24	1753.25	1761.92	1768.44	1766.68	1766.64	1768.70	1768.17	1766.25	1765.36	1765.60
Log Likelihood	-356.56	-358.46	-359.43	-358.89	-359.51	-358.86	-358.97	-354.81	-359.31	-358.78	-359.06	-351.56	-355.90	-359.16	-358.28	-358.25	-359.28	-359.02	-358.06	-357.62	-357.73
Deviance	713.12	716.92	718.85	717.79	719.01	717.71	717.94	709.62	718.62	717.56	718.11	703.12	711.79	718.31	716.56	716.51	718.57	718.04	716.13	715.23	715.47
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.02	−0.09*	0.09	0.14	0.17	0.45***	0.24***	0.02	−0.27***	0.37**	−0.27**	−0.16*	−0.41***	0.36*	−0.10	0.10	−0.06	0.19**	0.29***	0.53***	−0.04
	(0.14)	(0.05)	(0.08)	(0.08)	(0.14)	(0.13)	(0.07)	(0.14)	(0.05)	(0.12)	(0.10)	(0.08)	(0.12)	(0.15)	(0.12)	(0.18)	(0.08)	(0.07)	(0.08)	(0.11)	(0.04)
DoS attack (t-1)	1.99***	2.01***	1.98***	1.95***	1.99***	1.93***	1.97***	1.99***	1.97***	1.99***	1.98***	1.96***	1.97***	1.94***	1.98***	1.98***	1.99***	1.98***	1.94***	1.91***	1.99***
	(0.21)	(0.21)	(0.22)	(0.22)	(0.21)	(0.19)	(0.21)	(0.21)	(0.24)	(0.22)	(0.21)	(0.24)	(0.21)	(0.21)	(0.22)	(0.20)	(0.21)	(0.22)	(0.25)	(0.23)	(0.21)
AIC	974.95	973.90	974.66	973.20	975.16	967.60	968.34	975.04	969.64	971.38	973.57	972.39	967.72	970.13	974.71	974.72	974.65	973.31	968.16	966.30	974.52
BIC	1769.08	1768.03	1768.79	1767.33	1769.28	1761.72	1762.47	1769.17	1763.77	1765.51	1767.70	1766.52	1761.85	1764.26	1768.84	1768.85	1768.78	1767.44	1762.29	1760.43	1768.64
Log Likelihood	-359.48	-358.95	-359.33	-358.60	-359.58	-355.80	-356.17	-359.52	-356.82	-357.69	-358.78	-358.19	-355.86	-357.07	-359.36	-359.36	-359.33	-358.66	-356.08	-355.15	-359.26
Deviance	718.95	717.90	718.66	717.20	719.16	711.60	712.34	719.04	713.64	715.38	717.57	716.39	711.72	714.13	718.71	718.72	718.65	717.31	712.16	710.30	718.52
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.36: Penalized logistic regression results (5XX error codes) - medium-term models (newspaper and day fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	LeBat opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	−0.15	0.22***	−0.03	0.00	−0.14	0.02	0.06	0.17	−0.35*	−0.10	−0.00	0.04	0.12	−0.12	0.00	0.14	−0.10	0.06	−0.29	−0.18	−0.00	0.10**	−0.07
	(0.14)	(0.05)	(0.11)	(0.12)	(0.11)	(0.09)	(0.10)	(0.10)	(0.17)	(0.14)	(0.15)	(0.09)	(0.15)	(0.06)	(0.16)	(0.11)	(0.14)	(0.13)	(0.15)	(0.21)	(0.09)	(0.03)	(0.12)
Number of headlines	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.02	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.22***	2.12***	2.25***	2.25***	2.25***	2.25***	2.25***	2.21***	2.20***	2.25***	2.25***	2.25***	2.23***	2.24***	2.25***	2.23***	2.22***	2.24***	2.20***	2.26***	2.25***	2.25***	2.25***
	(0.27)	(0.28)	(0.26)	(0.25)	(0.26)	(0.25)	(0.26)	(0.27)	(0.26)	(0.26)	(0.25)	(0.26)	(0.26)	(0.26)	(0.26)	(0.26)	(0.26)	(0.26)	(0.26)	(0.27)	(0.25)	(0.25)	(0.25)
AIC	1242.76	1233.44	1245.42	1245.64	1243.13	1245.63	1245.08	1238.67	1235.26	1244.07	1245.63	1245.48	1243.11	1243.41	1245.64	1243.48	1244.26	1245.17	1230.10	1241.59	1245.63	1243.77	1244.77
BIC	1267.45	1258.14	1270.11	1270.34	1267.82	1270.32	1269.77	1263.36	1259.96	1268.76	1270.32	1270.18	1267.80	1268.10	1270.33	1268.18	1268.96	1269.87	1263.80	1266.69	1270.33	1268.47	1269.47
Log Likelihood	-617.38	-612.72	-618.71	-618.82	-617.56	-618.81	-618.54	-615.33	-613.63	-618.03	-618.81	-618.74	-617.55	-617.70	-618.82	-617.74	-618.13	-618.59	-615.55	-617.00	-618.82	-617.89	-618.39
Deviance	1234.76	1225.44	1237.42	1237.64	1235.13	1237.63	1237.08	1230.67	1227.26	1236.07	1237.63	1237.48	1235.11	1235.41	1237.64	1235.48	1236.26	1237.17	1231.10	1233.99	1237.63	1235.77	1236.77
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.03	0.08	0.08	0.20	0.14	−0.29**	0.00	0.12**	−0.20	0.05	−0.23	−0.02	0.07	0.07	0.09	−0.07	0.09	−0.15	0.07	0.11	−0.10	−0.11	0.09
	(0.12)	(0.12)	(0.07)	(0.12)	(0.10)	(0.11)	(0.12)	(0.04)	(0.16)	(0.07)	(0.21)	(0.05)	(0.06)	(0.12)	(0.08)	(0.17)	(0.09)	(0.13)	(0.09)	(0.09)	(0.08)	(0.09)	(0.06)
Number of headlines	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.25***	2.23***	2.25***	2.20***	2.22***	2.23***	2.25***	2.21***	2.21***	2.25***	2.21***	2.24***	2.24***	2.25***	2.24***	2.24***	2.25***	2.23***	2.24***	2.23***	2.24***	2.25***	2.23***
	(0.25)	(0.26)	(0.25)	(0.25)	(0.27)	(0.27)	(0.26)	(0.25)	(0.26)	(0.25)	(0.25)	(0.26)	(0.25)	(0.25)	(0.25)	(0.26)	(0.26)	(0.26)	(0.25)	(0.26)	(0.26)	(0.26)	(0.26)
AIC	1245.64	1244.68	1244.62	1236.98	1241.07	1239.32	1245.64	1241.05	1240.53	1245.35	1238.99	1245.48	1244.97	1244.98	1244.55	1244.84	1244.51	1242.44	1244.06	1243.34	1244.08	1243.68	1244.06
BIC	1270.34	1269.38	1269.32	1261.68	1265.76	1264.01	1270.33	1265.75	1265.22	1270.05	1263.69	1270.18	1269.67	1269.67	1269.25	1269.53	1269.21	1267.13	1269.66	1268.03	1268.78	1268.37	1268.75
Log Likelihood	-618.82	-618.34	-618.31	-614.49	-616.53	-615.66	-618.82	-616.53	-616.26	-618.68	-615.50	-618.74	-618.49	-618.49	-618.28	-618.42	-618.25	-617.22	-618.48	-617.67	-618.04	-617.84	-618.03
Deviance	1237.64	1236.68	1236.62	1228.98	1233.07	1231.32	1237.64	1233.05	1232.53	1237.35	1230.99	1237.48	1236.97	1236.98	1236.55	1236.84	1236.51	1234.44	1236.96	1235.34	1236.08	1235.68	1236.06
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.37: Penalized logistic regression results (incl. 999 error codes) - short-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.01	0.02	−0.15	0.03	−0.11	−0.01	−0.01	0.07	−0.31**	−0.05	0.01	−0.06	0.09	−0.08	−0.01	0.08	−0.13	0.10	0.07*	−0.05	−0.05
	(0.16)	(0.04)	(0.09)	(0.07)	(0.08)	(0.11)	(0.04)	(0.07)	(0.12)	(0.08)	(0.07)	(0.13)	(0.08)	(0.06)	(0.09)	(0.08)	(0.19)	(0.09)	(0.04)	(0.10)	(0.10)
DoS attack (t-1)	1.33***	1.32***	1.32***	1.32***	1.34***	1.33***	1.32***	1.33***	1.31***	1.33***	1.33***	1.31***	1.32***	1.33***	1.33***	1.31***	1.30***	1.32***	1.33***	1.33***	1.33***
	(0.25)	(0.24)	(0.23)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.27)	(0.24)	(0.24)	(0.24)	(0.25)	(0.25)	(0.25)	(0.24)	(0.25)	(0.25)
AIC	1132.59	1132.46	1129.74	1132.47	1131.18	1132.52	1132.48	1131.52	1129.59	1132.20	1132.55	1132.03	1131.48	1131.53	1132.55	1131.94	1131.24	1131.21	1131.54	1132.12	1132.19
BIC	1262.24	1262.11	1259.39	1262.12	1260.83	1262.17	1262.13	1261.17	1259.24	1261.86	1262.21	1261.68	1261.13	1261.18	1262.20	1261.59	1260.89	1260.86	1261.19	1261.77	1261.84
Log Likelihood	-545.29	-545.23	-543.87	-545.23	-544.59	-545.26	-545.24	-544.76	-543.80	-545.10	-545.28	-545.01	-544.74	-544.76	-545.27	-544.97	-544.62	-544.60	-544.77	-545.06	-545.09
Deviance	1090.59	1090.46	1087.74	1090.47	1089.18	1090.52	1090.48	1089.52	1087.59	1090.20	1090.55	1090.03	1089.48	1089.53	1090.55	1089.94	1089.24	1089.21	1089.54	1090.12	1090.19
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.07	0.05	0.30***	0.17***	−0.24**	−0.02	0.08*	−0.12	−0.13*	−0.08	0.05	0.01	0.06	0.03	−0.07	0.19*	0.00	0.01	0.02	−0.05	0.02
	(0.08)	(0.05)	(0.06)	(0.03)	(0.08)	(0.12)	(0.04)	(0.11)	(0.07)	(0.15)	(0.07)	(0.05)	(0.09)	(0.05)	(0.14)	(0.08)	(0.09)	(0.06)	(0.06)	(0.06)	(0.03)
DoS attack (t-1)	1.31***	1.33***	1.27***	1.30***	1.33***	1.33***	1.30***	1.31***	1.28***	1.32***	1.33***	1.33***	1.32***	1.32***	1.32***	1.33***	1.32***	1.32***	1.33***	1.33***	1.32***
	(0.25)	(0.24)	(0.28)	(0.25)	(0.24)	(0.24)	(0.26)	(0.24)	(0.25)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)
AIC	1132.05	1132.11	1121.77	1127.61	1129.49	1132.49	1130.62	1131.01	1130.03	1131.92	1132.43	1132.52	1132.18	1132.50	1132.00	1129.61	1132.55	1132.54	1132.50	1132.22	1132.44
BIC	1261.70	1261.76	1251.42	1257.26	1259.14	1262.14	1260.27	1260.66	1259.68	1261.58	1262.08	1262.17	1261.83	1262.15	1261.65	1259.26	1262.20	1262.19	1262.15	1261.87	1262.09
Log Likelihood	-545.03	-545.05	-539.89	-542.80	-543.74	-545.24	-544.31	-544.50	-544.01	-544.96	-545.21	-545.26	-545.09	-545.25	-545.00	-543.80	-545.28	-545.27	-545.25	-545.11	-545.22
Deviance	1090.05	1090.11	1079.77	1085.61	1087.49	1090.49	1088.62	1089.01	1088.03	1089.92	1090.43	1090.52	1090.18	1090.50	1090.00	1087.61	1090.55	1090.54	1090.50	1090.22	1090.44
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.38: Penalized logistic regression results (incl. 999 error codes) - short-term models (newspaper fixed effects). Note: Newspaper fixed are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.08	0.03	−0.18*	0.04	−0.14	−0.07	0.03	0.11	−0.30**	−0.06	−0.04	−0.03	0.14	−0.09*	−0.05	0.09	−0.04	0.07	0.04	−0.02	−0.07
	(0.16)	(0.05)	(0.08)	(0.09)	(0.09)	(0.11)	(0.04)	(0.07)	(0.12)	(0.10)	(0.10)	(0.11)	(0.07)	(0.05)	(0.11)	(0.06)	(0.17)	(0.08)	(0.05)	(0.08)	(0.10)
DoS attack (t-1)	1.14***	1.13***	1.12***	1.13***	1.15***	1.13***	1.13***	1.14***	1.12***	1.13***	1.13***	1.12***	1.12***	1.13***	1.13***	1.12***	1.12***	1.13***	1.14***	1.13***	1.14***
	(0.25)	(0.25)	(0.24)	(0.25)	(0.25)	(0.25)	(0.25)	(0.24)	(0.25)	(0.25)	(0.25)	(0.27)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.24)	(0.26)	(0.25)
AIC	1161.04	1161.01	1157.78	1161.06	1159.27	1160.65	1161.03	1158.58	1158.39	1160.80	1161.00	1161.06	1158.96	1159.95	1160.89	1160.39	1161.06	1160.59	1160.91	1161.15	1160.68
BIC	1463.56	1463.53	1460.30	1463.58	1461.78	1463.17	1463.55	1461.10	1460.91	1463.32	1463.52	1463.58	1461.48	1462.47	1463.41	1462.91	1463.58	1463.11	1463.43	1463.67	1463.20
Log Likelihood	-531.52	-531.50	-529.89	-531.53	-530.63	-531.33	-531.51	-530.29	-530.19	-531.40	-531.50	-531.53	-530.48	-530.98	-531.45	-531.19	-531.53	-531.29	-531.46	-531.57	-531.34
Deviance	1063.04	1063.01	1059.78	1063.06	1061.27	1062.65	1063.03	1060.58	1060.39	1062.80	1063.00	1063.06	1060.96	1061.95	1062.89	1062.39	1063.06	1062.59	1062.91	1063.15	1062.68
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.07	0.02	0.28***	0.14***	−0.23**	−0.02	0.09**	−0.12	−0.17*	−0.14	0.05	0.01	0.07	0.10	−0.04	0.21*	−0.06	−0.01	0.02	−0.03	0.03
	(0.06)	(0.05)	(0.04)	(0.04)	(0.09)	(0.11)	(0.03)	(0.11)	(0.08)	(0.19)	(0.08)	(0.04)	(0.10)	(0.05)	(0.13)	(0.09)	(0.07)	(0.06)	(0.06)	(0.08)	(0.04)
DoS attack (t-1)	1.12***	1.13***	1.09***	1.11***	1.14***	1.13***	1.11***	1.12***	1.08***	1.13***	1.13***	1.13***	1.13***	1.13***	1.13***	1.13***	1.13***	1.13***	1.13***	1.14***	1.13***
	(0.25)	(0.25)	(0.27)	(0.26)	(0.25)	(0.25)	(0.26)	(0.25)	(0.26)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)	(0.25)
AIC	1160.72	1161.13	1153.23	1157.77	1158.68	1161.14	1159.04	1159.91	1157.56	1159.80	1161.03	1161.16	1160.79	1160.37	1161.06	1157.75	1160.78	1161.17	1161.14	1161.03	1161.03
BIC	1463.24	1463.65	1455.75	1460.29	1461.20	1463.65	1461.56	1462.42	1460.08	1462.32	1463.55	1463.68	1463.31	1462.88	1463.58	1460.27	1463.30	1463.69	1463.66	1463.54	1463.55
Log Likelihood	-531.36	-531.57	-527.61	-529.88	-530.34	-531.57	-530.52	-530.95	-529.78	-530.90	-531.52	-531.58	-531.39	-531.18	-531.53	-529.87	-531.39	-531.58	-531.57	-531.51	-531.52
Deviance	1062.72	1063.13	1055.23	1059.77	1060.68	1063.14	1061.04	1061.91	1059.56	1061.80	1063.03	1063.16	1062.79	1062.37	1063.06	1059.75	1062.78	1063.17	1063.14	1063.03	1063.03
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.39: Penalized logistic regression results (incl. 999 error codes) - short-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.04	0.05	−0.17	0.02	−0.15	−0.06	−0.00	0.09	−0.35***	−0.09	−0.09	−0.04	0.19*	−0.05	−0.04	0.07	−0.00	0.04	0.03	0.05	−0.03
	(0.16)	(0.05)	(0.09)	(0.10)	(0.09)	(0.09)	(0.04)	(0.06)	(0.11)	(0.07)	(0.11)	(0.11)	(0.08)	(0.05)	(0.07)	(0.07)	(0.13)	(0.10)	(0.06)	(0.07)	(0.07)
DoS attack (t-1)	1.35***	1.35***	1.33***	1.35***	1.37***	1.34***	1.35***	1.35***	1.33***	1.35***	1.35***	1.34***	1.34***	1.34***	1.34***	1.34***	1.35***	1.35***	1.35***	1.34***	1.35***
	(0.19)	(0.18)	(0.18)	(0.19)	(0.19)	(0.19)	(0.19)	(0.18)	(0.19)	(0.19)	(0.19)	(0.20)	(0.19)	(0.19)	(0.19)	(0.18)	(0.19)	(0.19)	(0.18)	(0.20)	(0.19)
AIC	1217.01	1216.59	1214.25	1216.95	1214.88	1216.69	1216.93	1215.53	1213.05	1216.39	1216.30	1216.75	1212.51	1216.60	1216.90	1216.48	1217.06	1216.79	1216.86	1216.74	1216.87
BIC	2155.44	2155.02	2152.67	2155.37	2153.31	2155.11	2155.36	2153.95	2151.47	2154.82	2154.72	2155.17	2150.94	2155.03	2155.32	2154.90	2155.48	2155.22	2155.28	2155.16	2155.30
Log Likelihood	-456.51	-456.30	-455.12	-456.47	-455.44	-456.34	-456.47	-455.76	-454.52	-456.20	-456.15	-456.37	-454.26	-456.30	-456.45	-456.24	-456.53	-456.40	-456.43	-456.37	-456.44
Deviance	913.01	912.59	910.25	912.95	910.88	912.69	912.93	911.53	909.05	912.39	912.30	912.75	908.51	912.60	912.90	912.48	913.06	912.79	912.86	912.74	912.87
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.01	0.04	0.29***	0.15***	−0.24***	0.10	0.16***	−0.01	−0.18**	−0.22	0.06	0.03	0.04	0.16**	−0.02	0.31***	−0.18*	−0.02	−0.00	−0.03	0.06
	(0.07)	(0.05)	(0.06)	(0.04)	(0.07)	(0.11)	(0.04)	(0.09)	(0.07)	(0.15)	(0.06)	(0.03)	(0.10)	(0.05)	(0.12)	(0.09)	(0.07)	(0.07)	(0.06)	(0.06)	(0.05)
DoS attack (t-1)	1.35***	1.35***	1.32***	1.33***	1.36***	1.35***	1.30***	1.35***	1.29***	1.36***	1.35***	1.35***	1.34***	1.33***	1.35***	1.35***	1.37***	1.35***	1.35***	1.35***	1.35***
	(0.19)	(0.18)	(0.21)	(0.19)	(0.19)	(0.19)	(0.21)	(0.18)	(0.18)	(0.19)	(0.18)	(0.18)	(0.18)	(0.19)	(0.19)	(0.19)	(0.19)	(0.19)	(0.19)	(0.19)	(0.19)
AIC	1216.99	1216.75	1208.92	1213.72	1213.99	1216.17	1211.73	1217.05	1212.54	1213.79	1216.86	1216.86	1216.86	1214.52	1217.00	1209.65	1214.02	1216.96	1216.94	1216.91	1216.34
BIC	2155.41	2155.18	2147.35	2152.15	2152.42	2154.59	2150.16	2155.48	2150.97	2152.22	2155.28	2155.29	2155.28	2152.95	2155.42	2148.07	2152.45	2155.39	2155.37	2155.33	2154.76
Log Likelihood	-456.49	-456.38	-452.46	-454.86	-455.00	-456.08	-453.87	-456.53	-454.27	-454.90	-456.43	-456.43	-456.43	-455.26	-456.50	-452.82	-455.01	-456.48	-456.47	-456.45	-456.17
Deviance	912.99	912.75	904.92	909.72	909.99	912.17	907.73	913.05	908.54	909.79	912.86	912.86	912.86	910.52	913.00	905.65	910.02	912.96	912.94	912.91	912.34
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.40: Penalized logistic regression results (incl. 999 error codes) - short-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	−0.29	0.21***	0.05	−0.06	0.01	−0.03	−0.01	0.20**	−0.34	−0.15	0.08	−0.04	0.14	−0.27	0.07	0.20	−0.24	0.11	−0.44*	−0.27	0.00	0.12*	−0.05
	(0.17)	(0.05)	(0.12)	(0.07)	(0.12)	(0.14)	(0.13)	(0.07)	(0.22)	(0.21)	(0.19)	(0.12)	(0.16)	(0.17)	(0.17)	(0.13)	(0.17)	(0.19)	(0.17)	(0.18)	(0.17)	(0.05)	(0.12)
Number of headlines	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.02	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.21***	2.16***	2.24***	2.25***	2.25***	2.24***	2.25***	2.16***	2.18***	2.22***	2.24***	2.25***	2.22***	2.22***	2.24***	2.22***	2.23***	2.24***	2.20***	2.23***	2.20***	2.19***	2.25***	2.22***	2.25***
	(0.27)	(0.26)	(0.26)	(0.25)	(0.26)	(0.26)	(0.26)	(0.28)	(0.26)	(0.26)	(0.26)	(0.26)	(0.27)	(0.27)	(0.26)	(0.26)	(0.27)	(0.28)	(0.26)	(0.26)	(0.25)	(0.25)	(0.25)
AIC	1240.56	1235.27	1245.13	1244.74	1245.48	1245.30	1245.43	1235.63	1235.11	1241.56	1244.44	1245.20	1241.97	1239.15	1244.54	1240.86	1238.76	1243.64	1235.29	1237.44	1245.47	1242.85	1244.97
BIC	1265.25	1259.96	1269.82	1269.44	1270.17	1269.99	1270.13	1260.32	1259.80	1266.65	1269.14	1269.89	1266.66	1263.84	1269.23	1265.56	1263.45	1268.34	1259.99	1262.13	1270.17	1267.34	1269.67
Log Likelihood	-616.28	-613.63	-618.57	-618.37	-618.74	-618.65	-618.72	-613.82	-613.55	-616.98	-618.22	-618.60	-616.98	-615.58	-618.27	-616.43	-615.38	-617.82	-613.65	-614.72	-618.74	-617.32	-618.49
Deviance	1232.56	1227.27	1237.13	1236.74	1237.48	1237.30	1237.43	1227.63	1227.11	1233.96	1236.44	1237.20	1233.97	1231.15	1236.54	1232.86	1230.76	1235.64	1227.29	1229.44	1237.47	1234.65	1236.97
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.01	0.08	−0.04	0.10	0.15	−0.28	0.06	0.10	−0.22	0.02	−0.16	−0.00	0.05	0.00	0.10	−0.02	0.05	−0.15	0.13	0.26*	−0.09	−0.08	0.04
	(0.12)	(0.14)	(0.08)	(0.11)	(0.16)	(0.17)	(0.12)	(0.06)	(0.19)	(0.09)	(0.17)	(0.05)	(0.08)	(0.15)	(0.08)	(0.16)	(0.12)	(0.14)	(0.13)	(0.13)	(0.08)	(0.11)	(0.11)
Number of headlines	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01	−0.01
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	2.24***	2.24***	2.25***	2.23***	2.20***	2.29**	2.24***	2.21***	2.21***	2.24***	2.21***	2.25***	2.24***	2.25***	2.24***	2.24***	2.24***	2.23***	2.23***	2.16**	2.24***	2.24***	2.24***
	(0.26)	(0.26)	(0.26)	(0.25)	(0.29)	(0.27)	(0.25)	(0.26)	(0.26)	(0.25)	(0.25)	(0.26)	(0.25)	(0.26)	(0.25)	(0.26)	(0.25)	(0.26)	(0.26)	(0.30)	(0.26)	(0.26)	(0.26)
AIC	1245.48	1244.58	1245.07	1243.83	1240.91	1239.35	1244.86	1243.53	1239.08	1245.43	1241.92	1245.47	1246.07	1245.48	1243.95	1245.38	1245.10	1242.21	1242.76	1239.86	1244.14	1244.48	1245.27
BIC	1270.17	1269.27	1269.76	1268.52	1265.60	1264.05	1269.56	1268.23	1263.77	1270.13	1266.62	1270.16	1269.76	1270.17	1268.65	1270.07	1269.79	1266.91	1267.46	1255.55	1268.84	1269.17	1269.97
Log Likelihood	-618.74	-618.29	-618.53	-617.91	-616.45	-615.68	-618.43	-617.77	-615.54	-618.72	-616.96	-618.73	-618.53	-618.74	-617.98	-618.69	-618.55	-617.11	-617.38	-611.43	-618.07	-618.24	-618.64
Deviance	1237.48	1236.58	1237.07	1235.83	1232.91	1231.35	1236.86	1235.53	1231.08	1237.43	1233.92	1237.47	1237.07	1237.48	1235.95	1237.38	1237.10	1234.21	1234.76	1222.86	1236.14	1236.48	1237.27
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.4.41: Penalized logistic regression results (incl. 999 error codes) - medium-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.15	−0.11	−0.09	−0.02	0.08	−0.24	−0.11***	0.05	−0.25	−0.09	0.10	−0.15	0.12*	0.01	−0.21	0.12	−0.10	0.15	0.13**	0.02	−0.12
	(0.26)	(0.06)	(0.10)	(0.08)	(0.08)	(0.14)	(0.03)	(0.03)	(0.25)	(0.09)	(0.09)	(0.20)	(0.06)	(0.06)	(0.14)	(0.13)	(0.16)	(0.09)	(0.05)	(0.08)	(0.11)
DoS attack (t-1)	1.58***	1.57***	1.59***	1.59***	1.59***	1.59***	1.58***	1.59***	1.58***	1.58***	1.59***	1.57***	1.58***	1.59***	1.57***	1.58***	1.59***	1.58***	1.57***	1.59***	1.59***
	(0.36)	(0.36)	(0.33)	(0.34)	(0.34)	(0.32)	(0.34)	(0.34)	(0.35)	(0.34)	(0.34)	(0.39)	(0.34)	(0.34)	(0.34)	(0.37)	(0.34)	(0.34)	(0.32)	(0.34)	(0.34)
AIC	1237.07	1235.48	1236.91	1237.75	1237.42	1232.20	1235.62	1237.34	1236.84	1236.76	1236.96	1235.72	1236.22	1237.87	1235.16	1236.53	1236.59	1235.73	1234.13	1237.83	1236.72
BIC	1367.36	1365.77	1367.20	1368.03	1367.71	1362.49	1365.90	1367.63	1367.13	1367.05	1367.25	1366.01	1366.51	1368.16	1365.44	1366.82	1366.88	1366.02	1364.42	1368.11	1367.01
Log Likelihood	-597.53	-596.74	-597.46	-597.87	-597.71	-595.10	-596.81	-597.67	-597.42	-597.38	-597.48	-596.86	-597.11	-597.93	-596.58	-597.27	-597.29	-596.86	-596.07	-597.91	-597.36
Deviance	1195.07	1193.48	1194.91	1195.75	1195.42	1190.20	1193.62	1195.34	1194.84	1194.76	1194.96	1193.72	1194.22	1195.87	1193.16	1194.53	1194.59	1193.73	1192.13	1195.83	1194.72
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.08	−0.05	0.10*	0.18**	−0.20**	0.12	0.04	−0.05	−0.21***	0.17	0.13	−0.05	−0.10	0.04	0.00	0.18*	0.10	0.07	0.19	0.06	−0.03
	(0.15)	(0.05)	(0.04)	(0.06)	(0.06)	(0.15)	(0.03)	(0.12)	(0.06)	(0.11)	(0.07)	(0.10)	(0.11)	(0.08)	(0.11)	(0.09)	(0.08)	(0.14)	(0.11)	(0.09)	(0.02)
DoS attack (t-1)	1.59***	1.59***	1.58***	1.55***	1.58***	1.58***	1.58***	1.59***	1.55***	1.60***	1.59***	1.58***	1.58**	1.59***	1.59***	1.59***	1.58***	1.59**	1.56***	1.59***	1.59***
	(0.34)	(0.34)	(0.34)	(0.35)	(0.33)	(0.35)	(0.34)	(0.33)	(0.35)	(0.33)	(0.33)	(0.36)	(0.34)	(0.34)	(0.34)	(0.33)	(0.33)	(0.35)	(0.39)	(0.34)	(0.34)
AIC	1237.34	1237.19	1237.10	1232.96	1234.82	1236.92	1237.60	1237.57	1231.26	1236.10	1236.35	1237.32	1237.06	1237.79	1237.92	1235.86	1236.52	1237.44	1232.66	1237.51	1237.47
BIC	1367.63	1367.48	1367.39	1363.25	1365.11	1367.21	1367.88	1367.86	1361.55	1366.39	1366.64	1367.60	1367.35	1368.07	1368.21	1366.15	1366.81	1367.73	1362.95	1367.80	1367.76
Log Likelihood	-597.67	-597.60	-597.55	-595.48	-596.41	-597.46	-597.80	-597.79	-594.63	-597.05	-597.18	-597.66	-597.53	-597.89	-597.96	-596.93	-597.26	-597.72	-595.33	-597.75	-597.73
Deviance	1195.34	1195.19	1195.10	1190.96	1192.82	1194.92	1195.60	1195.57	1189.26	1194.10	1194.35	1195.32	1195.06	1195.79	1195.92	1193.86	1194.52	1195.44	1190.66	1195.51	1195.47
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.42: Penalized logistic regression results (incl. 999 error codes) - medium-term models (newspaper fixed effects). Note: Newspaper effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.05	−0.08	0.02	−0.08	0.09	−0.26	−0.17***	0.11*	−0.36	−0.17	0.03	−0.12	0.29***	0.02	−0.34*	0.13	−0.08	0.17	0.11*	0.03	−0.10
	(0.21)	(0.05)	(0.11)	(0.09)	(0.08)	(0.15)	(0.05)	(0.05)	(0.27)	(0.12)	(0.11)	(0.19)	(0.07)	(0.05)	(0.13)	(0.13)	(0.16)	(0.11)	(0.06)	(0.06)	(0.12)
DoS attack (t-1)	1.41***	1.40***	1.41***	1.41***	1.41***	1.40***	1.39***	1.40***	1.39***	1.39***	1.41***	1.39***	1.37***	1.41***	1.38***	1.39***	1.41***	1.40***	1.40***	1.41***	1.41***
	(0.35)	(0.36)	(0.35)	(0.35)	(0.35)	(0.34)	(0.37)	(0.36)	(0.36)	(0.36)	(0.35)	(0.38)	(0.35)	(0.35)	(0.36)	(0.37)	(0.35)	(0.35)	(0.34)	(0.36)	(0.35)
AIC	1266.20	1265.23	1266.12	1265.36	1265.62	1260.82	1262.53	1264.25	1264.14	1263.87	1266.05	1264.78	1258.24	1266.03	1260.61	1264.97	1265.63	1263.76	1264.06	1266.04	1265.63
BIC	1570.20	1569.23	1570.13	1569.37	1569.62	1564.83	1566.54	1568.25	1568.14	1567.87	1570.05	1568.79	1562.24	1570.03	1564.61	1568.97	1569.63	1567.77	1568.06	1570.04	1569.63
Log Likelihood	-584.10	-583.62	-584.06	-583.68	-583.81	-581.41	-582.27	-583.13	-583.07	-582.93	-584.02	-583.39	-580.12	-584.01	-581.30	-583.49	-583.82	-582.88	-583.03	-584.02	-583.81
Deviance	1168.20	1167.23	1168.12	1167.36	1167.62	1162.82	1164.53	1166.25	1166.14	1165.87	1168.05	1166.78	1160.24	1168.03	1162.61	1166.97	1167.63	1165.76	1166.06	1168.04	1167.63
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.05	−0.06	0.05	0.17*	−0.20**	0.16	0.05	−0.10	−0.26***	0.13	0.11	−0.05	−0.12	0.21	0.13	0.20*	0.10	−0.05	0.19	0.15	−0.03
	(0.18)	(0.05)	(0.06)	(0.08)	(0.08)	(0.16)	(0.04)	(0.12)	(0.06)	(0.13)	(0.10)	(0.09)	(0.11)	(0.13)	(0.09)	(0.08)	(0.12)	(0.14)	(0.11)	(0.10)	(0.04)
DoS attack (t-1)	1.41***	1.41***	1.41***	1.38***	1.40**	1.40***	1.40***	1.41***	1.35***	1.41**	1.41***	1.41***	1.40***	1.40***	1.41***	1.40**	1.40***	1.41***	1.38***	1.39***	1.41***
	(0.35)	(0.35)	(0.35)	(0.36)	(0.35)	(0.36)	(0.35)	(0.35)	(0.36)	(0.35)	(0.34)	(0.36)	(0.35)	(0.36)	(0.35)	(0.34)	(0.34)	(0.35)	(0.38)	(0.36)	(0.35)
AIC	1266.00	1265.51	1265.90	1262.62	1263.31	1264.79	1265.59	1265.33	1257.20	1265.42	1265.04	1265.96	1264.97	1263.16	1265.29	1263.87	1265.38	1265.94	1261.81	1264.26	1265.84
BIC	1570.00	1569.52	1569.90	1566.62	1567.31	1568.80	1569.59	1569.33	1561.20	1569.42	1569.05	1569.96	1568.97	1567.17	1569.29	1567.88	1569.38	1569.94	1565.81	1568.26	1569.85
Log Likelihood	-584.00	-583.76	-583.95	-582.31	-582.66	-583.40	-583.79	-583.66	-579.60	-583.71	-583.52	-583.98	-583.48	-582.58	-583.65	-582.94	-583.69	-583.97	-581.90	-583.13	-583.92
Deviance	1168.00	1167.51	1167.90	1164.62	1165.31	1166.79	1167.59	1167.33	1159.20	1167.42	1167.04	1167.96	1166.97	1165.16	1167.29	1165.87	1167.38	1167.94	1163.81	1166.26	1167.84
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.43: Penalized logistic regression results (incl. 999 error codes) - medium-term models (newspaper and week fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.01	−0.07	0.07	−0.07	0.05	−0.23	−0.19***	0.16***	−0.34	−0.19	0.05	−0.13	0.37***	0.05	−0.30*	0.22	−0.07	0.16	0.14**	0.01	−0.10
	(0.22)	(0.04)	(0.11)	(0.07)	(0.08)	(0.13)	(0.04)	(0.05)	(0.20)	(0.10)	(0.11)	(0.17)	(0.07)	(0.05)	(0.12)	(0.12)	(0.11)	(0.12)	(0.05)	(0.04)	(0.11)
DoS attack (t-1)	1.61***	1.59***	1.61***	1.61***	1.61***	1.60***	1.59***	1.58***	1.59***	1.58***	1.61***	1.59***	1.59***	1.61***	1.58***	1.58***	1.61***	1.59***	1.60***	1.61***	1.60***
	(0.24)	(0.25)	(0.23)	(0.24)	(0.24)	(0.23)	(0.25)	(0.25)	(0.25)	(0.25)	(0.24)	(0.27)	(0.23)	(0.24)	(0.25)	(0.26)	(0.24)	(0.24)	(0.23)	(0.24)	(0.24)
AIC	1307.37	1306.53	1306.91	1306.50	1307.16	1303.01	1302.16	1303.05	1305.46	1304.65	1307.14	1305.70	1295.60	1306.92	1302.83	1303.96	1306.99	1305.18	1304.24	1307.27	1306.77
BIC	2256.60	2255.76	2256.14	2255.73	2256.39	2252.24	2251.39	2252.28	2254.69	2253.88	2256.37	2254.94	2244.84	2256.15	2252.06	2253.19	2256.23	2254.42	2253.47	2256.50	2256.01
Log Likelihood	-500.68	-500.26	-500.45	-500.25	-500.58	-498.51	-498.08	-498.52	-499.73	-499.33	-500.57	-499.85	-494.80	-500.46	-498.42	-498.98	-500.50	-499.59	-499.12	-500.63	-500.39
Deviance	1001.37	1000.53	1000.91	1000.50	1001.16	997.01	996.16	997.05	999.46	998.65	1001.14	999.70	989.60	1000.92	996.83	997.96	1000.99	999.18	998.24	1001.27	1000.77
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.03	−0.12**	0.08	0.12	−0.19**	0.09	0.08	−0.05	−0.29***	0.11	0.10	−0.02	−0.13	0.17	0.13	0.23*	0.01	−0.03	0.22*	0.14	−0.05
	(0.14)	(0.04)	(0.05)	(0.08)	(0.06)	(0.14)	(0.06)	(0.11)	(0.03)	(0.13)	(0.08)	(0.09)	(0.09)	(0.11)	(0.09)	(0.09)	(0.11)	(0.13)	(0.10)	(0.08)	(0.03)
DoS attack (t-1)	1.61***	1.61***	1.60***	1.58***	1.60***	1.60***	1.60***	1.61***	1.54***	1.61***	1.60***	1.60***	1.60**	1.59***	1.61***	1.60**	1.61***	1.61***	1.57***	1.58**	1.60***
	(0.24)	(0.23)	(0.24)	(0.24)	(0.24)	(0.24)	(0.24)	(0.23)	(0.24)	(0.24)	(0.23)	(0.25)	(0.24)	(0.25)	(0.24)	(0.23)	(0.23)	(0.24)	(0.27)	(0.25)	(0.24)
AIC	1307.28	1304.97	1306.87	1305.53	1304.52	1306.83	1306.16	1307.07	1295.48	1306.82	1306.35	1307.14	1305.78	1305.33	1306.50	1303.87	1307.28	1307.23	1301.91	1305.69	1306.68
BIC	2256.51	2254.20	2256.10	2254.76	2253.75	2256.06	2255.39	2256.30	2244.72	2256.05	2255.58	2256.37	2255.01	2254.56	2255.73	2253.10	2256.51	2256.46	2251.14	2254.92	2255.91
Log Likelihood	-500.64	-499.49	-500.44	-499.77	-499.26	-500.41	-500.08	-500.53	-494.74	-500.41	-500.17	-500.57	-499.89	-499.66	-500.25	-498.93	-500.64	-500.61	-497.95	-499.84	-500.34
Deviance	1001.28	998.97	1000.87	999.53	998.52	1000.83	1000.16	1001.07	989.48	1000.82	1000.35	1001.14	999.78	999.33	1000.50	997.87	1001.28	1001.23	995.91	999.69	1000.68
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.44: Penalized logistic regression results (incl. 999 error codes) - medium-term models (newspaper and day fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	LeBlat opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.34	0.06	−0.30*	0.34**	0.17	−0.39	−0.23	−0.62	0.02	0.56**	0.06	−0.42***	0.37	−1.48*	−0.36	0.21*	0.15	−0.70	0.04	−1.32	0.41	−0.03	0.19*
	(0.20)	(0.19)	(0.15)	(0.05)	(0.09)	(0.29)	(0.37)	(0.55)	(0.24)	(0.19)	(0.20)	(0.11)	(0.19)	(0.65)	(0.25)	(0.09)	(0.19)	(0.37)	(0.15)	(1.17)	(0.22)	(0.21)	(0.09)
Number of headlines	0.06***	0.07***	0.07***	0.07***	0.07***	0.07***	0.08***	0.07***	0.07***	0.08***	0.07***	0.09***	0.07***	0.08***	0.07***	0.06**	0.07***	0.07***	0.07***	0.07**	0.08***	0.07***	0.07***
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	3.04**	3.17***	3.20***	3.26***	3.17***	3.39***	3.08***	3.11***	3.19***	2.99***	3.17***	2.91***	2.93***	3.06***	3.13***	3.08***	3.18***	3.05***	3.19***	3.12***	3.20***	3.18***	3.23***
	(0.67)	(0.73)	(0.75)	(0.70)	(0.69)	(0.74)	(0.83)	(0.75)	(0.73)	(0.86)	(0.76)	(0.78)	(0.86)	(0.70)	(0.74)	(0.70)	(0.73)	(0.78)	(0.74)	(0.75)	(0.72)	(0.73)	(0.75)
AIC	201.17	201.88	200.86	200.14	201.91	200.41	201.00	199.63	201.89	196.51	201.91	198.10	199.50	198.40	200.67	200.17	201.87	198.51	202.01	197.33	200.38	201.76	202.02
BIC	225.87	226.57	225.56	224.84	226.61	225.10	225.69	224.32	226.59	221.20	226.60	222.80	224.20	223.10	225.37	224.87	226.57	223.20	226.71	222.02	225.07	226.46	226.72
Log Likelihood	-96.58	-96.94	-96.43	-96.07	-96.96	-96.20	-96.50	-95.81	-96.95	-94.25	-96.95	-95.05	-95.75	-95.20	-96.34	-96.09	-96.94	-95.25	-97.00	-94.66	-96.19	-96.88	-97.01
Deviance	193.17	193.88	192.86	192.14	193.91	192.41	193.00	191.63	193.89	188.51	193.91	190.10	191.50	190.40	192.67	192.17	193.87	190.51	194.01	189.33	192.38	193.76	194.02
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.35**	0.09	0.03	0.35	−0.42**	0.18	−0.27	0.26**	0.48	−0.36	0.58***	−0.37*	−0.53	0.18	0.50**	0.40***	−0.12	0.31*	−0.52	0.07	0.14	0.13	−0.74*
	(0.11)	(0.21)	(0.22)	(0.19)	(0.15)	(0.12)	(0.26)	(0.07)	(0.28)	(0.25)	(0.16)	(0.15)	(0.27)	(0.26)	(0.16)	(0.08)	(0.16)	(0.15)	(0.67)	(0.25)	(0.10)	(0.13)	(0.31)
Number of headlines	0.07***	0.07***	0.07***	0.07***	0.08***	0.07***	0.07***	0.07***	0.08***	0.07***	0.06**	0.08***	0.07***	0.07***	0.08***	0.08***	0.08***	0.07***	0.07***	0.07***	0.07***	0.07***	0.08***
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	3.11***	3.17***	3.18***	3.06***	3.10***	3.17***	3.20***	3.16***	3.19***	3.12***	3.18***	3.15***	3.08***	3.16***	3.04***	3.21***	3.14***	3.06***	3.12***	3.18***	3.19***	3.17***	3.03***
	(0.74)	(0.74)	(0.76)	(0.77)	(0.74)	(0.73)	(0.73)	(0.77)	(0.79)	(0.76)	(0.67)	(0.74)	(0.82)	(0.73)	(0.75)	(0.75)	(0.71)	(0.78)	(0.74)	(0.73)	(0.74)	(0.73)	(0.74)
AIC	199.92	201.83	201.84	200.76	199.78	202.43	201.00	202.10	199.35	200.59	197.48	200.60	199.44	201.73	197.38	199.62	201.46	200.76	200.19	201.93	202.27	201.91	198.76
BIC	224.62	226.52	226.53	225.45	224.47	227.13	225.70	226.80	224.05	225.29	222.18	225.29	224.14	226.42	222.08	224.31	226.16	225.46	224.88	226.62	226.96	226.60	223.46
Log Likelihood	-95.96	-96.91	-96.92	-96.38	-95.89	-97.22	-96.50	-97.05	-95.68	-96.30	-94.74	-96.30	-95.72	-96.86	-94.69	-95.81	-96.73	-96.38	-96.09	-96.96	-97.13	-96.95	-95.38
Deviance	191.92	193.83	193.84	192.76	191.78	194.43	193.00	194.10	191.35	192.59	189.48	192.60	191.44	193.73	189.38	191.62	193.46	192.76	192.19	193.93	194.27	193.91	190.76
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.45: Penalized logistic regression results (strong attacks) - short-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.65**	0.48***	−0.21**	0.30***	−0.18	−0.14	0.02	−0.72*	−0.36*	0.59**	0.03	−0.03	0.37***	−0.42*	−0.22	−0.76**	−1.79*	0.42**	0.25***	0.26**	0.21*
	(0.24)	(0.10)	(0.07)	(0.03)	(0.11)	(0.10)	(0.16)	(0.36)	(0.39)	(0.10)	(0.11)	(0.09)	(0.07)	(0.17)	(0.17)	(0.23)	(0.82)	(0.14)	(0.07)	(0.07)	(0.08)
DoS attack (t-1)	2.67***	2.53***	2.64***	2.65***	2.62***	2.62***	2.61***	2.55***	2.49***	2.50***	2.61***	2.61***	2.51***	2.59***	2.59***	2.62***	2.59***	2.63***	2.61***	2.64***	2.62***
	(0.45)	(0.47)	(0.49)	(0.44)	(0.51)	(0.46)	(0.48)	(0.50)	(0.54)	(0.60)	(0.47)	(0.47)	(0.51)	(0.46)	(0.46)	(0.51)	(0.46)	(0.47)	(0.46)	(0.48)	(0.47)
AIC	225.36	226.06	226.59	225.92	226.37	227.01	227.24	224.94	225.52	221.58	227.25	227.17	225.93	226.22	226.65	224.72	220.98	225.94	227.70	227.25	226.91
BIC	354.91	355.71	356.24	355.57	356.02	356.66	356.89	354.59	355.17	351.23	356.90	356.82	355.58	355.87	356.31	354.37	350.63	355.59	357.35	356.90	356.56
Log Likelihood	-91.63	-92.03	-92.29	-91.96	-92.19	-92.51	-92.62	-91.47	-91.76	-89.79	-92.62	-92.58	-91.96	-92.11	-92.33	-91.36	-89.49	-91.97	-92.85	-92.63	-92.45
Deviance	183.26	184.06	184.59	183.92	184.37	185.01	185.24	182.94	183.52	179.58	185.25	185.17	183.93	184.22	184.65	182.72	178.98	183.94	185.70	185.25	184.91
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.07	0.07	0.68***	−0.07	0.28***	−1.12***	0.25***	0.43*	−0.39	0.95***	−0.22*	−0.60***	0.17	0.57***	0.36***	0.31***	0.33***	−0.93**	0.34***	0.26***	−0.74***
	(0.18)	(0.11)	(0.12)	(0.11)	(0.04)	(0.26)	(0.04)	(0.20)	(0.23)	(0.16)	(0.10)	(0.10)	(0.23)	(0.09)	(0.10)	(0.07)	(0.08)	(0.36)	(0.09)	(0.07)	(0.19)
DoS attack (t-1)	2.62***	2.62***	2.55***	2.61***	2.60***	2.43***	2.60***	2.65***	2.56***	2.67***	2.61***	2.62***	2.62***	2.52***	2.69***	2.62***	2.52***	2.50***	2.61***	2.59***	2.56***
	(0.46)	(0.46)	(0.45)	(0.46)	(0.47)	(0.49)	(0.50)	(0.54)	(0.53)	(0.46)	(0.48)	(0.54)	(0.47)	(0.46)	(0.49)	(0.46)	(0.49)	(0.41)	(0.46)	(0.47)	(0.48)
AIC	227.03	227.39	224.24	227.04	227.66	221.01	227.69	225.66	226.27	218.86	226.79	224.97	227.36	221.10	225.82	226.88	226.48	223.83	227.29	227.18	224.93
BIC	356.68	357.04	353.89	356.69	357.31	350.66	357.34	355.31	355.92	348.51	356.44	354.62	357.01	350.75	355.47	356.53	356.13	353.48	356.94	356.83	354.58
Log Likelihood	-92.52	-92.70	-91.12	-92.52	-92.83	-89.50	-92.85	-91.83	-92.13	-88.43	-92.40	-91.48	-92.68	-89.55	-91.91	-92.44	-92.24	-90.91	-92.64	-92.59	-91.47
Deviance	185.03	185.39	182.24	185.04	185.66	179.01	185.69	183.66	184.27	176.86	184.79	182.97	185.36	179.10	183.82	184.88	184.48	181.83	185.29	185.18	182.93
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.46: Penalized logistic regression results (strong attacks) - short-term models (newspaper fixed effects). Note: Newspaper fixed are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−0.07***	0.26*	−0.55***	0.14***	−0.42***	−0.30***	0.18	−0.74	−0.75**	0.51***	−0.04	−0.18*	0.17**	0.02	−0.05	−0.27	−1.66*	0.70***	0.01	0.34**	0.48***
	(0.22)	(0.11)	(0.15)	(0.03)	(0.07)	(0.06)	(0.10)	(0.39)	(0.26)	(0.11)	(0.06)	(0.08)	(0.06)	(0.13)	(0.13)	(0.28)	(0.77)	(0.17)	(0.13)	(0.08)	(0.11)
DoS attack (t-1)	1.60***	1.53**	1.53**	1.56***	1.54**	1.57**	1.56**	1.45*	1.45**	1.56**	1.54**	1.53**	1.54**	1.55**	1.54**	1.58**	1.59***	1.54***	1.55**	1.58**	1.52**
	(0.46)	(0.48)	(0.55)	(0.47)	(0.50)	(0.48)	(0.48)	(0.57)	(0.52)	(0.55)	(0.48)	(0.48)	(0.48)	(0.48)	(0.48)	(0.50)	(0.48)	(0.45)	(0.48)	(0.51)	(0.50)
AIC	227.43	229.31	227.50	229.18	227.03	228.86	229.62	227.37	228.16	226.03	229.44	229.07	229.39	229.55	229.41	229.26	224.40	226.44	229.55	228.89	227.89
BIC	437.34	439.22	437.41	439.09	436.94	438.78	439.53	437.28	438.08	435.94	439.35	438.98	439.30	439.46	439.32	439.17	434.31	436.35	439.46	438.80	437.80
Log Likelihood	-79.72	-80.66	-79.75	-80.59	-79.52	-80.43	-80.81	-79.69	-80.08	-79.02	-80.72	-80.54	-80.69	-80.77	-80.71	-80.63	-78.20	-79.22	-80.77	-80.44	-79.95
Deviance	159.43	161.31	159.50	161.18	159.03	160.86	161.62	159.37	160.16	158.03	161.44	161.07	161.39	161.55	161.41	161.26	156.40	158.44	161.55	160.89	159.89
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.29**	−0.10	0.69***	−0.06	−0.03	−1.26***	0.46***	0.51***	0.14	0.95***	−0.28*	−0.41***	0.20	0.47***	0.85***	0.35***	0.05	−0.65***	0.36***	−0.06	−0.59***
	(0.09)	(0.08)	(0.07)	(0.08)	(0.13)	(0.22)	(0.05)	(0.13)	(0.10)	(0.08)	(0.13)	(0.11)	(0.20)	(0.07)	(0.11)	(0.08)	(0.08)	(0.23)	(0.10)	(0.08)	(0.15)
DoS attack (t-1)	1.49**	1.55**	1.48**	1.54**	1.55**	1.39**	1.55**	1.54**	1.55**	1.64**	1.55**	1.60**	1.56**	1.51**	1.60***	1.54**	1.54**	1.47***	1.53**	1.53**	1.52**
	(0.50)	(0.49)	(0.51)	(0.48)	(0.48)	(0.46)	(0.50)	(0.57)	(0.47)	(0.51)	(0.48)	(0.54)	(0.49)	(0.47)	(0.48)	(0.47)	(0.48)	(0.41)	(0.48)	(0.49)	(0.48)
AIC	229.48	229.04	226.23	229.34	229.55	221.71	229.45	226.08	229.82	221.52	228.80	228.18	229.57	225.49	222.82	228.97	229.47	227.30	229.33	229.33	227.89
BIC	439.39	438.95	436.15	439.25	439.46	431.62	439.36	435.99	439.74	431.43	438.72	438.09	439.48	435.40	432.73	438.88	439.38	437.22	439.24	439.24	437.80
Log Likelihood	-80.74	-80.52	-79.12	-80.67	-80.78	-76.86	-80.72	-79.04	-80.91	-76.76	-80.40	-80.09	-80.78	-78.75	-77.41	-80.48	-80.74	-79.65	-80.67	-80.66	-79.94
Deviance	161.48	161.04	158.23	161.34	161.55	153.71	161.45	158.08	161.82	153.52	160.80	160.18	161.57	157.49	154.82	160.97	161.47	159.30	161.33	161.33	159.89
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.47: Penalized logistic regression results (strong attacks) - short-term models (newspaper and week fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−1.36***	−0.07	−1.09***	0.61***	−0.13**	−1.43***	0.21	−0.31*	−0.25	0.61***	−0.06	−0.18***	0.04	0.14	−0.26*	0.18	−0.43	0.65***	−0.30*	0.55***	0.51***
	(0.27)	(0.14)	(0.16)	(0.04)	(0.04)	(0.21)	(0.12)	(0.13)	(0.13)	(0.09)	(0.13)	(0.05)	(0.06)	(0.12)	(0.11)	(0.16)	(0.22)	(0.16)	(0.13)	(0.10)	(0.10)
DoS attack (t-1)	3.17***	2.97***	2.95***	2.95***	2.88***	3.37***	2.97***	2.92***	2.96***	2.93***	2.96***	2.90***	2.96***	2.97***	2.96***	2.92***	2.94***	2.72***	3.01***	3.02***	2.91***
	(0.34)	(0.55)	(0.58)	(0.52)	(0.55)	(0.37)	(0.54)	(0.57)	(0.56)	(0.53)	(0.55)	(0.56)	(0.56)	(0.54)	(0.59)	(0.55)	(0.56)	(0.50)	(0.59)	(0.53)	(0.50)
AIC	171.64	178.06	172.68	175.68	177.75	173.12	178.09	177.61	177.86	175.03	178.03	177.13	178.12	178.19	177.56	178.28	177.20	175.27	177.35	176.95	177.77
BIC	424.77	431.19	425.81	428.81	430.88	426.25	431.22	430.74	430.98	428.16	431.16	430.26	431.25	431.32	430.69	431.41	430.33	428.40	430.48	430.08	430.89
Log Likelihood	-44.82	-48.03	-45.34	-46.84	-47.88	-45.56	-48.05	-47.80	-47.93	-46.52	-48.02	-47.57	-48.06	-48.10	-47.78	-48.14	-47.69	-46.63	-47.68	-47.47	-47.88
Deviance	89.64	96.06	90.68	93.68	95.75	91.12	96.09	95.61	95.86	93.03	96.03	95.13	96.12	96.19	95.56	96.28	95.20	93.27	95.35	94.95	95.77
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.21	0.28*	0.67***	0.08	−0.31	−0.70**	0.56***	0.45***	0.22	0.79***	−1.86***	−0.31*	0.17	0.54***	0.81***	0.37**	−0.19**	−0.53**	0.18**	0.04	−1.18***
	(0.14)	(0.13)	(0.15)	(0.11)	(0.17)	(0.27)	(0.04)	(0.13)	(0.12)	(0.08)	(0.52)	(0.12)	(0.18)	(0.08)	(0.06)	(0.10)	(0.07)	(0.18)	(0.07)	(0.15)	(0.22)
DoS attack (t-1)	2.90***	2.94***	2.88***	2.94***	2.99***	2.86***	3.07***	3.38***	2.93***	2.86***	3.56***	3.00***	2.94***	2.92***	2.95***	2.95***	2.95***	2.86***	2.93***	2.94***	2.76***
	(0.58)	(0.55)	(0.56)	(0.57)	(0.56)	(0.51)	(0.54)	(0.55)	(0.56)	(0.63)	(0.63)	(0.56)	(0.55)	(0.56)	(0.55)	(0.51)	(0.56)	(0.50)	(0.54)	(0.54)	(0.56)
AIC	177.82	178.16	174.96	178.17	177.37	175.89	177.07	174.47	178.23	172.25	172.31	177.37	177.87	172.57	172.65	176.64	177.56	176.21	177.88	178.12	174.04
BIC	430.94	431.29	428.09	431.29	430.50	429.02	430.20	427.59	431.36	425.37	425.44	430.50	431.00	425.70	425.78	429.76	430.69	429.34	431.01	431.25	427.17
Log Likelihood	-47.91	-48.08	-46.48	-48.08	-47.68	-46.95	-47.53	-46.23	-48.11	-45.12	-45.16	-47.69	-47.94	-45.29	-45.33	-47.32	-47.78	-47.11	-47.94	-48.06	-46.02
Deviance	95.82	96.16	92.96	96.17	95.37	93.89	95.07	92.47	96.23	90.25	90.31	95.37	95.87	90.57	90.65	94.64	95.56	94.21	95.88	96.12	92.04
Num. obs.	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547	3547

Table D.4.48: Penalized logistic regression results (strong attacks) - short-term models (newspaper and day fixed effects). Note: Newspaper and time fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled.

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Investment/infrastructure	Protest/shortages	Leftist opposition	Colombia border	Oscar Perez	Indigenous groups/diseases	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners
Topic	0.57***	−0.53*	−0.24	0.13	0.17	−0.14	−0.35	0.22	0.14	0.33*	0.04	−0.48*	0.53**	−1.69	−0.33	0.26***	0.44***	−0.32	0.08	0.44*	−0.10	−1.69	0.24
	(0.17)	(0.24)	(0.26)	(0.14)	(0.18)	(0.20)	(0.37)	(0.23)	(0.19)	(0.16)	(0.34)	(0.19)	(0.16)	(0.89)	(0.38)	(0.07)	(0.09)	(0.36)	(0.10)	(0.16)	(0.22)	(0.94)	(0.29)
Number of headlines	0.06***	0.07***	0.07***	0.07***	0.07***	0.07***	0.08**	0.07**	0.07***	0.08***	0.07**	0.09***	0.07***	0.08***	0.07***	0.05***	0.08***	0.07***	0.07***	0.08**	0.07**	0.07***	0.07***
	(0.01)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.03)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	3.07***	3.14***	3.17***	3.18***	3.19***	3.18**	3.02***	3.16***	3.19***	3.08***	3.17***	2.84***	2.79***	3.02***	3.11***	2.96***	3.12***	3.06***	3.19***	3.19**	3.19***	2.91***	3.20***
	(0.68)	(0.68)	(0.71)	(0.73)	(0.74)	(0.71)	(0.87)	(0.76)	(0.73)	(0.77)	(0.77)	(0.79)	(0.82)	(0.72)	(0.78)	(0.73)	(0.75)	(0.80)	(0.73)	(0.66)	(0.74)	(0.80)	(0.67)
AIC	198.23	199.75	203.18	201.90	201.88	201.35	200.24	202.06	202.04	200.70	201.86	197.54	195.75	198.61	200.85	198.51	200.42	200.24	202.16	200.48	201.67	195.45	201.34
BIC	222.92	224.45	225.87	226.59	226.57	226.04	224.93	226.75	226.73	225.39	226.56	222.24	220.45	223.30	225.54	223.20	225.12	224.94	226.85	225.17	226.37	220.14	226.03
Log Likelihood	-95.11	-95.88	-96.59	-96.95	-96.94	-96.67	-96.12	-97.03	-97.02	-96.35	-96.93	-94.77	-93.88	-95.30	-96.42	-95.25	-96.21	-96.12	-97.08	-96.24	-96.84	-93.72	-96.67
Deviance	190.23	191.75	193.18	193.90	193.88	193.35	192.24	194.06	194.04	192.70	193.86	189.54	187.75	190.61	192.85	190.51	192.42	192.24	194.16	192.48	193.67	187.45	193.34
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

	Russia	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Recession	Corruption	Education studies
Topic	0.32	0.09	−0.25	0.14	−0.09	0.19	0.50*	0.23*	0.31**	−0.52**	0.38	−0.63	0.01	0.24	0.24	0.24	−0.63**	0.39	−0.05	−0.33	0.15	0.36**	−0.58
	(0.18)	(0.25)	(0.13)	(0.11)	(0.15)	(0.12)	(0.22)	(0.09)	(0.13)	(0.19)	(0.25)	(0.40)	(0.30)	(0.21)	(0.14)	(0.20)	(0.23)	(0.20)	(0.36)	(0.28)	(0.10)	(0.11)	(0.40)
Number of headlines	0.07***	0.07***	0.08***	0.07***	0.07***	0.07***	0.08***	0.09***	0.08**	0.07***	0.06**	0.08***	0.07***	0.08***	0.07***	0.07***	0.10***	0.07***	0.07***	0.07***	0.07***	0.07**	0.08***
	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)
DoS attack (t-1)	3.07***	3.19***	3.09***	3.16***	3.17***	3.17***	3.14***	3.13***	3.16***	3.14***	3.15***	3.08***	3.17***	3.14***	3.11***	3.12***	3.03***	3.13***	3.19***	3.20**	3.19***	2.93***	3.01***
	(0.74)	(0.73)	(0.72)	(0.74)	(0.74)	(0.73)	(0.68)	(0.76)	(0.65)	(0.71)	(0.71)	(0.71)	(0.80)	(0.77)	(0.78)	(0.78)	(0.66)	(0.79)	(0.75)	(0.72)	(0.74)	(0.77)	(0.77)
AIC	200.60	201.81	200.60	202.06	201.56	202.19	199.21	201.50	200.74	200.01	200.48	200.09	201.82	201.49	201.69	201.98	197.96	201.41	201.78	200.90	202.26	199.55	199.72
BIC	225.29	226.51	225.29	226.75	226.25	226.88	223.91	226.19	225.43	224.70	225.17	224.78	226.51	226.18	226.38	226.68	222.65	226.10	226.48	225.59	226.95	224.24	224.41
Log Likelihood	-96.30	-96.91	-96.30	-97.03	-96.78	-97.10	-95.61	-96.75	-96.37	-96.00	-96.24	-96.04	-96.91	-96.75	-96.84	-96.99	-94.98	-96.70	-96.89	-96.45	-97.13	-95.78	-95.86
Deviance	192.60	193.81	192.60	194.06	193.56	194.19	191.21	193.50	192.74	192.01	192.48	192.09	193.82	193.49	193.69	193.98	189.96	193.41	193.78	192.90	194.26	191.55	191.72
Num. obs.	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545	3545

Table D.4.49: Penalized logistic regression results (strong attacks) - medium-term models (pooled). Note: Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.23	0.07	0.05	0.07	−0.70	0.15	−0.06	0.47**	−1.33***	0.30**	0.02	−0.12	0.89***	−0.38	0.32***	−0.03	0.84***	−0.92***	−1.96**	0.37**	0.06
	(0.16)	(0.07)	(0.09)	(0.15)	(0.42)	(0.09)	(0.22)	(0.16)	(0.22)	(0.09)	(0.22)	(0.30)	(0.14)	(0.30)	(0.05)	(0.12)	(0.17)	(0.26)	(0.69)	(0.12)	(0.14)
DoS attack (t-1)	2.81***	2.77***	2.77***	2.76***	2.62***	2.77***	2.77***	2.75***	2.66***	2.71***	2.77***	2.77***	2.61***	2.74***	2.78***	2.76***	2.69***	2.76***	2.60***	2.72***	2.77***
	(0.39)	(0.39)	(0.39)	(0.40)	(0.50)	(0.41)	(0.41)	(0.41)	(0.42)	(0.39)	(0.39)	(0.40)	(0.41)	(0.41)	(0.40)	(0.40)	(0.28)	(0.35)	(0.46)	(0.34)	(0.39)
AIC	230.21	229.88	229.95	229.81	226.76	229.99	229.69	228.95	228.48	229.23	229.80	229.68	223.24	229.10	229.70	229.49	225.87	227.17	224.21	229.08	229.66
BIC	360.49	360.17	360.23	360.10	357.05	360.28	359.98	359.24	358.77	359.52	360.08	359.97	353.52	359.38	359.99	359.78	356.16	357.46	354.49	359.36	359.95
Log Likelihood	-94.10	-93.94	-93.97	-93.91	-92.38	-94.00	-93.85	-93.48	-93.24	-93.62	-93.90	-93.84	-90.62	-93.55	-93.85	-93.75	-91.94	-92.59	-91.10	-93.54	-93.83
Deviance	188.21	187.88	187.95	187.81	184.76	187.99	187.69	186.95	186.48	187.23	187.80	187.68	181.24	187.10	187.70	187.49	183.87	185.17	182.21	187.08	187.66
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	−0.31	−0.56**	−0.23	0.65***	0.50***	0.26	0.17**	0.17	−0.85***	0.67***	−0.14	0.31**	0.28*	0.24***	−0.32	−0.05	0.05	−0.55***	−0.05	0.77***	0.07
	(0.37)	(0.18)	(0.13)	(0.18)	(0.10)	(0.29)	(0.06)	(0.15)	(0.20)	(0.21)	(0.11)	(0.10)	(0.12)	(0.05)	(0.30)	(0.17)	(0.13)	(0.15)	(0.13)	(0.14)	(0.17)
DoS attack (t-1)	2.70***	2.72***	2.77***	2.66***	2.78***	2.80***	2.75***	2.78***	2.71***	2.71***	2.76***	2.79***	2.78**	2.74***	2.80***	2.77***	2.77***	2.74***	2.78***	2.35***	2.79***
	(0.43)	(0.37)	(0.40)	(0.43)	(0.38)	(0.37)	(0.41)	(0.36)	(0.42)	(0.37)	(0.39)	(0.38)	(0.40)	(0.41)	(0.38)	(0.40)	(0.39)	(0.39)	(0.39)	(0.52)	(0.40)
AIC	229.06	227.77	229.52	227.24	229.39	229.75	229.79	229.62	227.86	227.44	229.76	229.55	229.87	229.68	228.84	229.56	229.74	228.79	229.82	221.87	230.21
BIC	359.34	358.05	359.81	357.53	359.67	360.03	360.07	359.91	358.14	357.73	360.04	359.84	360.16	359.97	359.12	359.85	360.03	359.08	360.10	352.15	360.49
Log Likelihood	-93.53	-92.88	-93.76	-92.62	-93.69	-93.87	-93.89	-93.81	-92.93	-92.72	-93.88	-93.78	-93.94	-93.84	-93.42	-93.78	-93.87	-93.39	-93.91	-89.93	-94.10
Deviance	187.06	185.77	187.52	185.24	187.39	187.75	187.79	187.62	185.86	185.44	187.76	187.55	187.87	187.68	186.84	187.56	187.74	186.79	187.82	179.87	188.21
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.50: Penalized logistic regression results (strong attacks) - medium-term models (newspaper fixed effects). Note: Newspaper effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	0.07	−0.35*	−1.07***	−0.67***	−0.75	0.12	0.32***	0.34**	−0.21	0.04	−0.99**	−0.21	0.85***	0.80***	0.68***	0.80**	2.37***	−0.95***	−2.99***	0.54***	0.01
	(0.21)	(0.15)	(0.25)	(0.14)	(0.41)	(0.07)	(0.04)	(0.11)	(0.16)	(0.15)	(0.22)	(0.26)	(0.13)	(0.08)	(0.13)	(0.05)	(0.26)	(0.19)	(0.54)	(0.09)	(0.17)
DoS attack (t-1)	1.69***	1.67***	1.52**	1.72**	1.58***	1.68***	1.66***	1.69***	1.67***	1.68***	1.64***	1.67***	1.69***	1.70***	1.65***	1.68**	1.49**	1.71***	1.55***	1.58***	1.68***
	(0.42)	(0.42)	(0.45)	(0.42)	(0.43)	(0.43)	(0.42)	(0.42)	(0.42)	(0.41)	(0.42)	(0.43)	(0.34)	(0.44)	(0.44)	(0.43)	(0.36)	(0.46)	(0.41)	(0.38)	(0.42)
AIC	232.51	231.73	229.18	229.36	230.27	232.35	231.72	231.91	232.26	232.34	229.73	232.01	228.48	232.65	229.57	230.97	221.16	230.29	225.35	230.51	232.12
BIC	443.45	442.67	440.12	440.30	441.21	443.29	442.66	442.85	443.20	443.28	440.67	442.95	439.42	443.59	440.51	441.91	432.10	441.23	436.29	441.45	443.06
Log Likelihood	-82.25	-81.86	-80.59	-80.68	-81.14	-82.18	-81.86	-81.96	-82.13	-82.17	-80.87	-82.01	-80.24	-82.33	-80.78	-81.48	-76.58	-81.15	-78.68	-81.26	-82.06
Deviance	164.51	163.73	161.18	161.36	162.27	164.35	163.72	163.91	164.26	164.34	161.73	164.01	160.48	164.65	161.57	162.97	153.16	162.29	157.35	162.51	164.12
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.29***	−0.00	−0.06	0.63***	−0.12	0.58*	0.30***	0.24***	0.30***	1.16**	−0.03	1.79***	0.02	−0.92***	0.16	0.16	−0.64***	−0.36*	−0.78***	0.70**	0.19***
	(0.07)	(0.17)	(0.12)	(0.17)	(0.20)	(0.23)	(0.05)	(0.06)	(0.06)	(0.38)	(0.10)	(0.12)	(0.12)	(0.15)	(0.09)	(0.21)	(0.15)	(0.15)	(0.23)	(0.10)	(0.04)
DoS attack (t-1)	1.69***	1.68***	1.68***	1.57**	1.67***	1.68***	1.66***	1.64***	1.69***	1.51***	1.69***	1.61***	1.69***	1.64***	1.66***	1.67***	1.68***	1.67***	1.67***	1.60***	1.70***
	(0.42)	(0.42)	(0.42)	(0.48)	(0.44)	(0.39)	(0.40)	(0.40)	(0.44)	(0.44)	(0.42)	(0.38)	(0.43)	(0.42)	(0.42)	(0.44)	(0.44)	(0.39)	(0.38)	(0.44)	(0.43)
AIC	232.05	232.14	232.27	229.43	232.22	231.35	231.69	231.69	232.42	227.87	232.47	223.56	232.34	229.12	232.42	232.31	230.77	231.69	230.32	229.48	232.55
BIC	442.99	443.08	443.21	440.37	443.16	442.29	442.63	442.63	443.36	438.81	443.41	434.50	443.28	440.06	443.36	443.25	441.71	442.63	441.26	440.42	443.49
Log Likelihood	-82.02	-82.07	-82.14	-80.72	-82.11	-81.68	-81.85	-81.84	-82.21	-79.93	-82.23	-77.78	-82.17	-80.56	-82.21	-82.15	-81.38	-81.84	-81.16	-80.74	-82.27
Deviance	164.05	164.14	164.27	161.43	164.22	163.35	163.69	163.69	164.42	159.87	164.47	155.56	164.34	161.12	164.42	164.31	162.77	163.69	162.32	161.48	164.55
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.51: Penalized logistic regression results (strong attacks) - medium-term models (newspaper and week fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

	General opinion	Salary/prices	Food policy	Exiled opposition	Court sentences	Economy policy	Child mortality	Outages	Weather	Election	Government-Opposition dialog	Music/entertainment	Government ministers	Protest/shortages	Colombia border	Oscar Perez	Church/Job offer (mixed)	National assembly	Airline (opening/closing)	Political Prisoners	Russia
Topic	−1.17*	−0.19*	−1.97***	−0.54***	−0.17	0.06	0.23***	0.26*	−0.20	0.18	−0.41***	−0.08	0.88***	0.80***	0.30***	0.88***	0.60***	−0.41**	−0.61***	0.28***	−0.73**
	(0.51)	(0.08)	(0.34)	(0.11)	(0.28)	(0.06)	(0.05)	(0.12)	(0.12)	(0.12)	(0.09)	(0.19)	(0.12)	(0.12)	(0.06)	(0.04)	(0.12)	(0.15)	(0.18)	(0.07)	(0.25)
DoS attack (t-1)	2.87***	2.95***	2.62***	2.88***	2.94***	2.98***	2.95***	2.94***	2.96***	2.96***	2.99***	2.97***	2.76**	2.92***	2.94***	2.99***	2.88***	2.96***	2.89***	2.96***	2.88***
	(0.44)	(0.52)	(0.58)	(0.57)	(0.54)	(0.54)	(0.54)	(0.52)	(0.52)	(0.50)	(0.51)	(0.55)	(0.42)	(0.50)	(0.53)	(0.52)	(0.50)	(0.52)	(0.53)	(0.51)	(0.45)
AIC	176.42	178.34	170.14	176.73	178.32	178.67	178.20	178.11	178.47	178.46	177.54	178.52	173.55	179.74	177.98	177.09	174.86	177.92	177.43	177.78	176.63
BIC	430.79	432.71	424.51	431.10	432.69	433.04	432.57	432.48	432.84	432.83	431.90	432.89	427.92	434.11	432.35	431.46	429.23	432.29	431.80	432.15	431.00
Log Likelihood	-47.21	-48.17	-44.07	-47.36	-48.16	-48.33	-48.10	-48.05	-48.24	-48.23	-47.77	-48.26	-45.77	-48.87	-47.99	-47.55	-46.43	-47.96	-47.71	-47.89	-47.31
Deviance	94.42	96.34	88.14	94.73	96.32	96.67	96.20	96.11	96.47	96.46	95.54	96.52	91.55	97.74	95.98	95.09	92.86	95.92	95.43	95.78	94.63
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

	Sanctions	Military	Cryptomoney	Shortages healthcare	Regulations	USA/Korea	Cuba	International Organizations	Exchange Rate	Maduro	Work opinion	Migration crisis	Petroleum	PDVSA	Resignations	Mining/Sport (mixed)	Opposition candidate	Earthquake/accidents	Shortages	Corruption	Education studies
Topic	0.27***	0.07	0.35**	0.37*	−0.06	0.15	0.68***	0.29***	0.18***	1.43***	−0.02	0.66***	−0.20	−0.13	0.17***	0.17	−0.39**	−0.29*	−0.82***	0.30**	0.13***
	(0.05)	(0.11)	(0.11)	(0.16)	(0.15)	(0.27)	(0.11)	(0.06)	(0.05)	(0.21)	(0.07)	(0.18)	(0.11)	(0.16)	(0.04)	(0.23)	(0.14)	(0.14)	(0.24)	(0.09)	(0.04)
DoS attack (t-1)	2.98***	2.98***	2.99***	2.73***	2.99***	2.93***	3.02***	2.96***	3.00***	2.76***	2.98***	2.76***	2.90***	2.93***	3.00***	2.96**	2.99**	2.93***	2.88***	2.87***	3.00***
	(0.53)	(0.53)	(0.53)	(0.66)	(0.53)	(0.51)	(0.47)	(0.54)	(0.53)	(0.52)	(0.52)	(0.51)	(0.54)	(0.52)	(0.53)	(0.52)	(0.56)	(0.49)	(0.51)	(0.56)	(0.52)
AIC	177.62	178.56	178.23	177.17	178.58	178.47	174.54	177.37	178.73	170.88	178.66	175.23	178.30	177.92	178.57	178.53	177.59	177.92	176.24	177.54	178.65
BIC	431.99	432.93	432.60	431.54	432.95	432.84	428.90	431.74	433.10	425.25	433.03	429.60	432.66	432.29	432.94	432.90	431.96	432.29	430.61	431.91	433.02
Log Likelihood	-47.81	-48.28	-48.11	-47.59	-48.29	-48.24	-46.27	-47.68	-48.37	-44.44	-48.33	-46.62	-48.15	-47.96	-48.29	-48.27	-47.79	-47.96	-47.12	-47.77	-48.33
Deviance	95.62	96.56	96.23	95.17	96.58	96.47	92.54	95.37	96.73	88.88	96.66	93.23	96.30	95.92	96.57	96.53	95.59	95.92	94.24	95.54	96.65
Num. obs.	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656	3656

Table D.4.52: Penalized logistic regression results (strong attacks) - medium-term models (newspaper and day fixed effects). Note: Newspaper and time-fixed effects are not displayed. Clustered standard errors in parentheses. Topic variables are scaled. $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

D.5 Consequences of DoS Attacks

In this appendix, I discuss the approach of how I investigate whether DoS attacks also have an impact on the (non-)reporting on specific news. More precisely, I am interested in whether news websites stop to report on specific topics after an attack took place in the medium-term. Again, the panel structure enables to investigate this question more rigorously. In contrast, a simple before- and after comparison for the attacked website might be misleading. First, specific topics are responsible for the attack, thus they are reported more on and before the attack day, and naturally declining afterward. Second, simple global trends, i.e., events to report on, determine news cycles. More precisely, I build up small panels around each attack that include previous (14 days before) and later (7 days after) reporting about topics.[7] In order to not bias the control units, I leave out other websites that were attacked in the same period. Additionally, in some incidents attacks appear to be clustered. In these cases, I consider them belonging together. I define clustered attacks if they co-occur within five days as for the statistical analysis the "pre-treatment" period has to be long enough.

Methodology, I follow a recent approach proposed by Xu (2017) and employ the so-called generalized synthetic control method, a generalization of a difference-in-difference design, that does not require that control- and treatment units need to follow parallel trends in the absence of the treatment. An assumption, which is likely violated in my case as attacked websites report more about specific topics before the attack as this is the very reason for the DoS attack. Furthermore, in contrast to other synthetic control approaches, the model also works with missing data points, which are present when the website scraping failed. The main idea of the generalized synthetic control method is to create artificial counterfactual cases for the attacked websites, which follow the same trend before the attack, and then compare these cases with the actual observed outcome after the treatment. For this, the method creates a counterfactual for each treated unit using control group information based on linear interactive fixed effects models that include unit-specific intercepts interacted with time-varying coefficients (for more details see Xu, 2017). All models are run with two-way (website and day) fixed effects, cross-validation procedures to find the optimal number of factor loadings r (to predict the pre-treatment period), and parametric bootstraps to create levels of uncertainty around the estimates.[8]

To investigate whether there is a change in reporting, I run these models for each identified attack panel and every topic as dependent variable (27×50 models). Then, I check whether topic estimates for the attacked websites are significant ($p < 0.05$) for

[7] Sometimes, I have to shorten this period to ensure that attack periods on the same website do not overlap.

[8] I set r choosing from 1 to 5 because for some dependent variables and attack periods models without loading (r=0) do not work.

the whole attack period. Table D.5.1 summarizes the results.[9]

No.	Attacked website	Attack date	Significant topic changes (p<0.05)	Hoster
1	http://www.noticierovenevision.net/	2018-05-21	Not known (scraping did not work)	AMAZON
2	http://www.analitica.com/	2018-02-05	Colombia border	CLOUDFLARE
3	http://www.noticierodigital.com/	2018-05-21	None	CLOUDFLARE
4	https://canaldenoticia.com/	2018-01-10	None	DREAMHOST
5	https://canaldenoticia.com/	2017-12-10	Resignations	DREAMHOST
6	http://www.el-nacional.com/	2017-12-04 – 2017-12-06	Outages & Regulations	AMAZON
7	http://informe21.com/	2018-04-18	None	CLOUDFLARE
8	http://informe21.com/	2018-05-02 – 2018-05-03	General opinion	CLOUDFLARE
9	https://www.lapatilla.com/	2018-05-28	None	CLOUDFLARE
10	https://www.lapatilla.com/	2018-05-15	None	CLOUDFLARE
11	https://www.lapatilla.com/	2018-04-03 – 2018-04-04	Russia	CLOUDFLARE
12	https://www.lapatilla.com/	2018-02-09 – 2018-02-10	None	CLOUDFLARE
13	https://www.lapatilla.com/	2017-12-14	None	CLOUDFLARE
14	https://www.lapatilla.com/	2017-11-22	None	CLOUDFLARE
15	http://confirmado.com.ve/	2018-05-22	None	GO-DADDY
16	http://confirmado.com.ve/	2018-04-26	Economy policy & political prisoners	GO-DADDY
17	http://confirmado.com.ve/	2018-04-14	None	GO-DADDY
18	http://confirmado.com.ve/	2018-03-30	Election	GO-DADDY
19	http://confirmado.com.ve/	2018-03-03	Russia & PDVSA	GO-DADDY
20	http://confirmado.com.ve/	2018-01-29 – 2018-02-01	Food policy	GO-DADDY
21	http://confirmado.com.ve/	2018-01-07	Not known (too few observations beforehand)	GO-DADDY
22	http://confirmado.com.ve/	2017-11-15 – 2017-11-21 (with breaks)	Not known (too few observations beforehand)	GO-DADDY
23	https://www.aporrea.org/	2018-05-19	None	CLOUDFLARE
24	https://www.aporrea.org/	2018-02-10 – 2018-03-06 (with breaks)	Mining/sport (mixed)	CLOUDFLARE
25	https://www.aporrea.org/	2017-12-17	Cuba	CLOUDFLARE
26	https://www.aporrea.org/	2017-12-05 – 2017-12-06	None	CLOUDFLARE
27	https://www.aporrea.org/	2017-11-24 – 2017-11-27	None	CLOUDFLARE

Table D.5.1: Results of synthetic control runs for each attack period and website. Note: The order reflects the frequency of DoS attacks on the respective outlets.

The results show significant topic changes in 11 of 27 attack periods. However, the maximal number of topic changes per attack period is only two. Given that there could be hypothetical changes in 50 topics per attack period, it is relatively rare that there is a change in reporting after DoS attacks. Another observation is that while attacks on Cloudflare protected servers lead to a change in only 33% of the attack periods, there is a least a change in one topic for the other servers in 66% of the cases. The main explanation for this difference is due to the measurement of DoS attacks. As described in the main text, Cloudflare protected servers also respond with a 503 code when they are put under attack mode. Thus, in the most cases, these websites are not affected by an attack and still online.

Finally, I run the models for the attack periods with significant changes again to report the magnitude and direction of these changes and, more importantly, check whether the models' assumptions hold. More precisely, I investigate whether the actual attacked website and counterfactual follow a similar trend before the DoS attack and whether the approach by Xu (2017) is able to create reliable counterfactuals.[10] This endeavor may have failed due to the inability to create counterfactuals from the control set as they are completely different compared to the attacked websites. Having these pitfalls in mind, I sort the models' results along with their ability to predict the pre-treatment period,

[9] In the replication files, I report all results. I set the "treatment" DoS attack to t-1 as the data set-up ensured that content occurs before potential DoS attacks at t=t.

[10] Furthermore, I assume that attack periods are independent of each other and that no other event affected only the attacked website on the attack day. Assumptions that may not be valid but are necessary for the here proposed approach.

i.e., there should be no significant difference between the attacked website and synthetic control before the treatment.

In six cases the models can create a counterfactual that follows with acceptable variation a similar trend before the attack happened. Under acceptable variation I understand cases where the confidence intervals for the topic estimates are not different from 0 before the DoS attack. In general, all models display high levels of uncertainty and one should interpret the results as trends only. Figure D.5.1 displays that the website *confirmado.com.ve* reported less on the issue of *political prisoners* after the website got attacked on April 26, 2018, suggesting a chilling effect of DoS attacks on the reporting on this political sensitive issue. Similarly, the website *el-nacional.com* reported less on the topic *outages* after it reporting substantially on this issue before (see Figure D.5.2). On the other hand, the topic *food policy* increased after DoS attacks on *confirmado.com.ve* on January 29, 2018 (see Figure D.5.3). It appears that the outlet reported slightly more about government policy to ensure food supplies, an issue the outlet would not have reported on without being attacked. Somehow puzzling, attacks on the same website on March 02, 2018 lead to a decrease of the topic *Russia* (see Figure D.5.4). Since this topic is considerably correlated to the topic *sanctions* (see Figure D.1.2 in Appendix D.1) it may be that rather this explains the shown decrease because it is not entirely clear why news websites should report less on the topic *Russia*. The model for the attack period on the website *aporrea.org* from January 27 until March 13, 2018, highlights slightly more reporting on the topic *mining/sport (mixed)* (see Figure D.5.5). Here, it is not clear whether this means that the website reports more on non-political (about sport) or mining-related issues within Venezuela. While the latter would be counter-intuitive, it has to be noted that Cloudflare protects this website and they might not have been affected by these DoS attacks. Finally, developments of the topic *Cuba* after the same website got attacked on December 17, 2017, do not show significant changes (see Figure D.5.6).

In the other seven cases (Figures D.5.7 – D.5.14), the models display considerable difference between the attacked and counterfactual website before the attack. There remain two controversial cases. The first is the measured DoS attack against the website *canaldenoticia.com* on December 9, 2017 (see Figure D.5.7). Here, the website devoted a large share of their website to reports on the topic *resignations* before the DoS attack, and, according to the counterfactual, would have continued reporting more on this issue if there would not have been an attack. The second is the attack on the website *confirmado.com.ve* on March 30, 2018 (see Figure D.5.8). Here, the results suggest an increase in the topic *election* after the attack. While this appears counter-intuitive, the topic may not necessarily reflect critical content, particularly, as the attack did not happen around election dates.

In general, it seems that the in this study measured DoS attacks change the reporting of news in the short-term only rarely. There may be several explanations for this finding.

First, the measured DoS attacks are rather short in duration (see Figure D.1.1). Second, websites are protected by DoS mitigation services. In fact, the results show that if there is a change, it is rather unprotected websites that change their reporting. Finally, since previous content might have caused the attack, the website already reported less on this topic when the attack happened. Furthermore, the absence of consequences does not mean that the motivation to launch DoS attacks is not to change the behavior of the attacked news websites. Future research should investigate potential medium- and long-term consequences of DoS attacks on news and other websites to a greater extent.

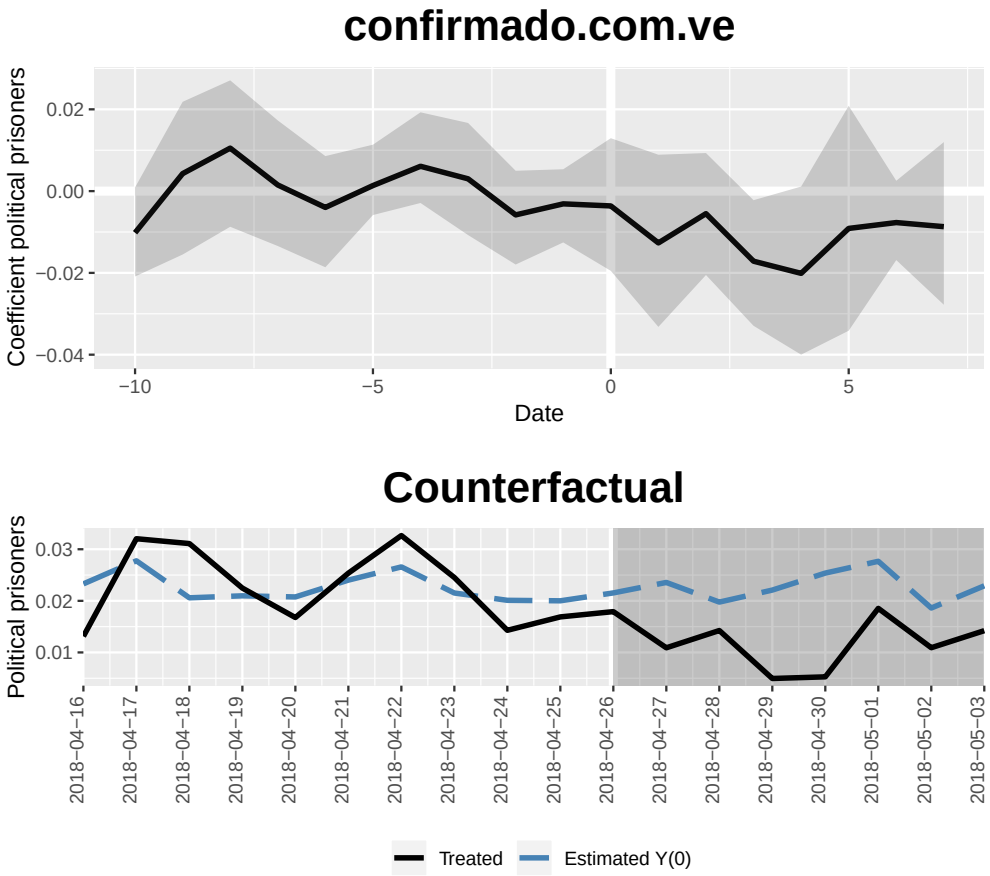

Figure D.5.1: Synthetic control model for DoS attack on confirmado.com.ve on 2018-04-26 showing the development of the topic *political prisoners*.

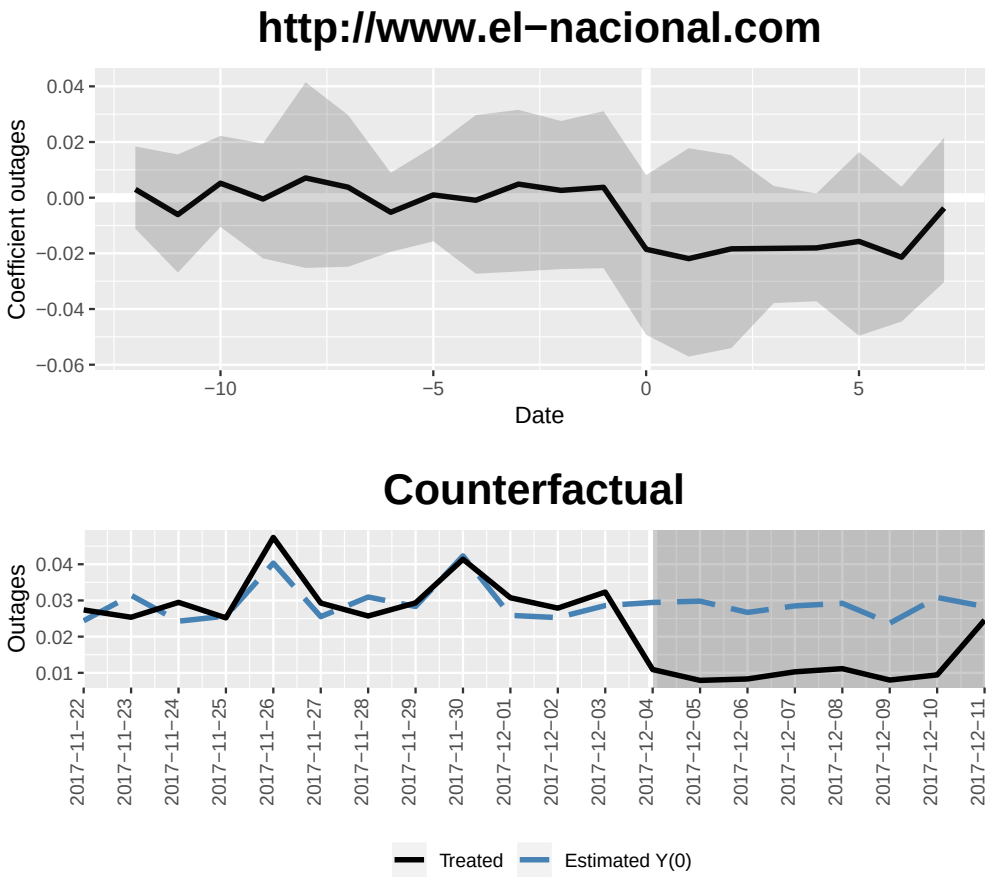

Figure D.5.2: Synthetic control model for DoS attack on el-nacional.com on 2017-12-04 showing the development of the topic *outages*.

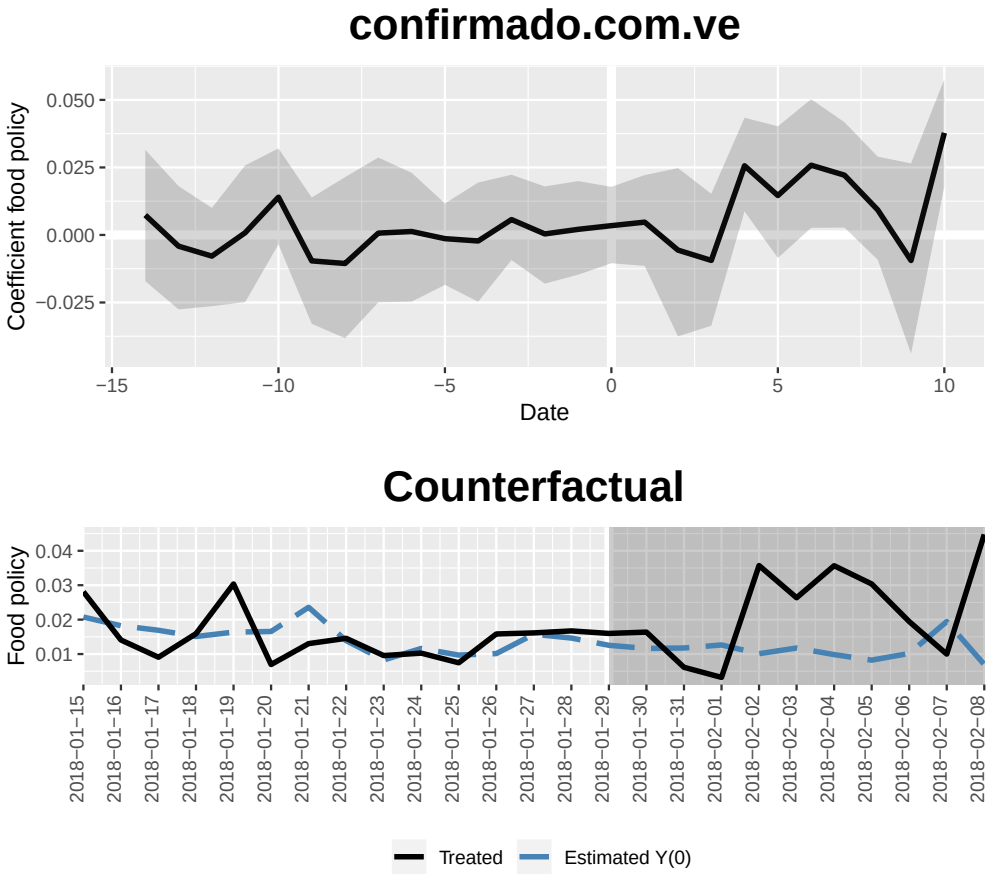

Figure D.5.3: Synthetic control model for DoS attack on confirmado.com.ve on 2018-01-29 showing the development of the topic *food policy*.

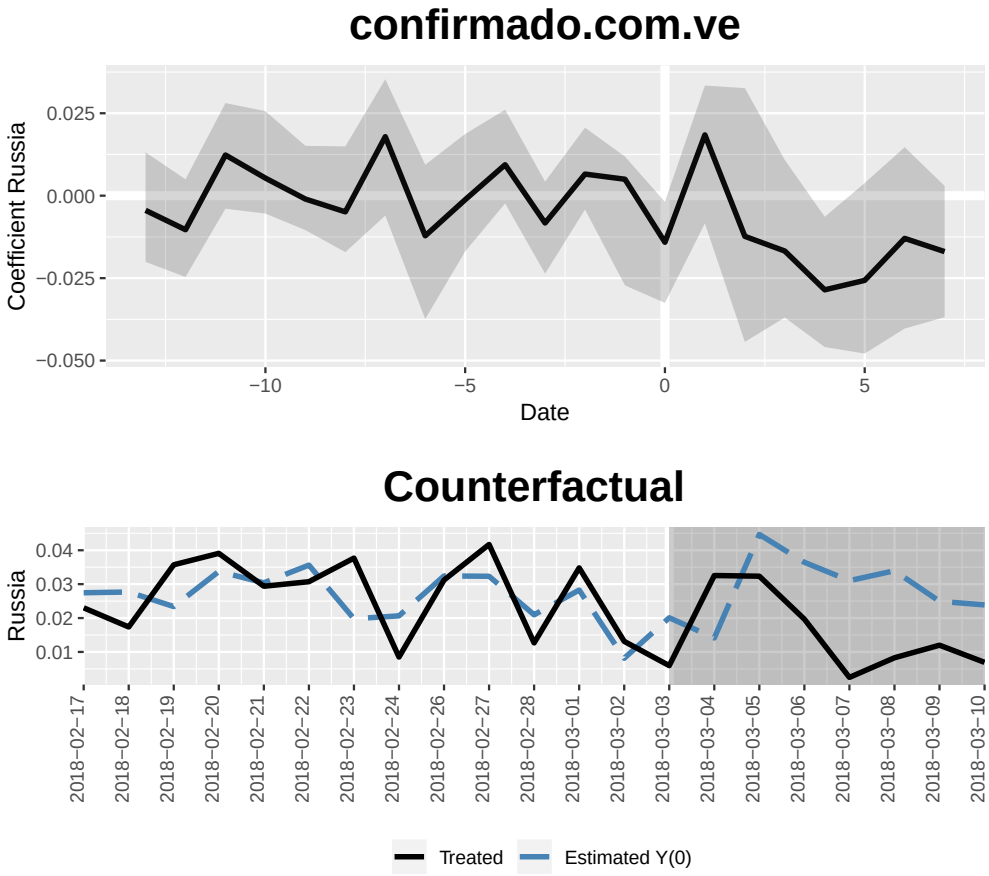

Figure D.5.4: Synthetic control model for DoS attack on confirmado.com.ve on 2018-03-03 showing the development of the topic *Russia*.

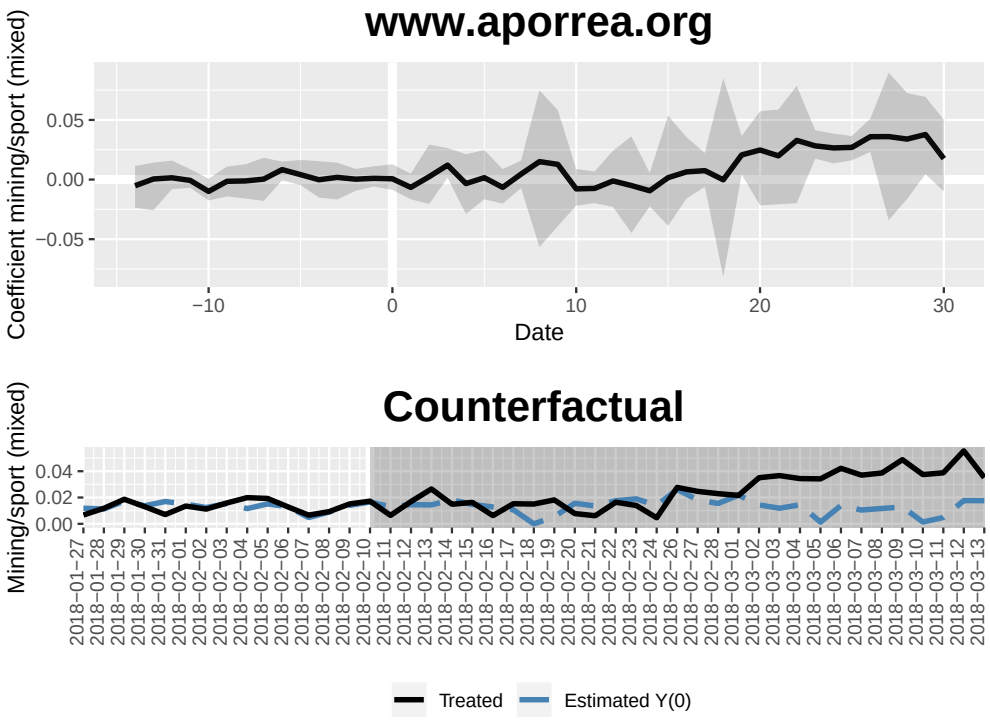

Figure D.5.5: Synthetic control model for DoS attack on aporrea.org on 2018-02-10 – 2018-03-06 showing the development of the topic *mining/sport (mixed)*. Note: There were multiple attacks in the period of study.

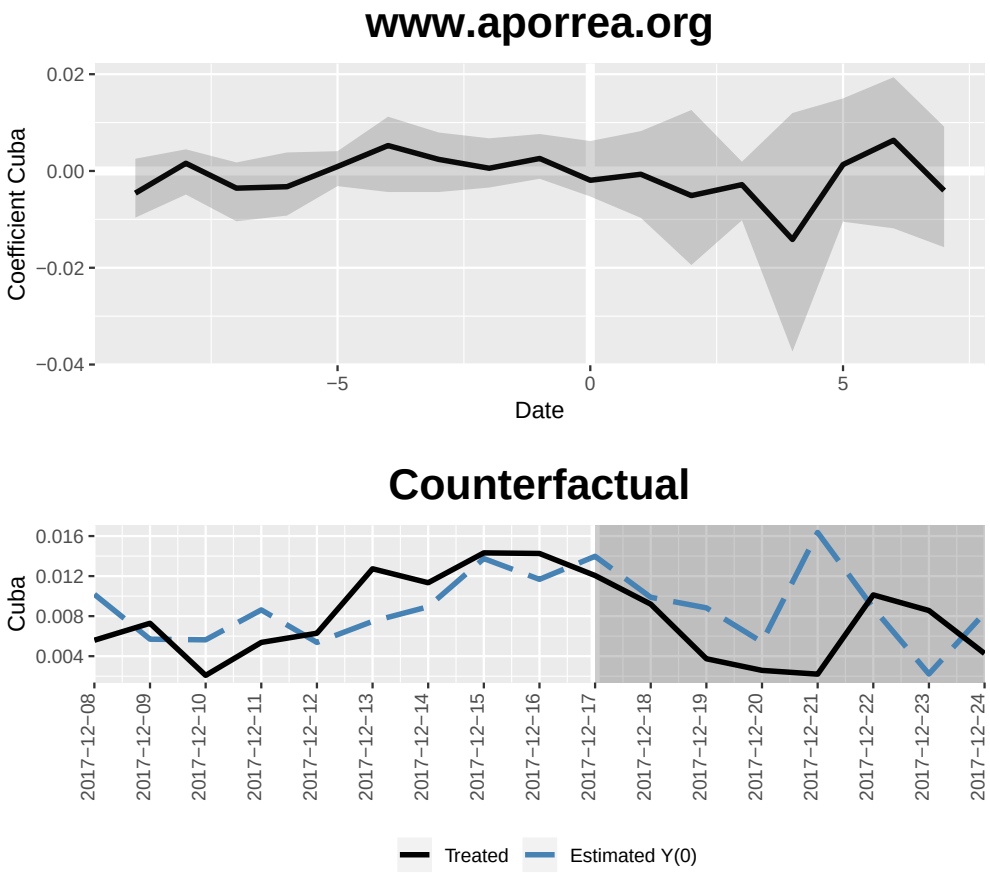

Figure D.5.6: Synthetic control model for DoS attack on aporrea.org on 2017-12-17 showing the development of the topic *Cuba*.

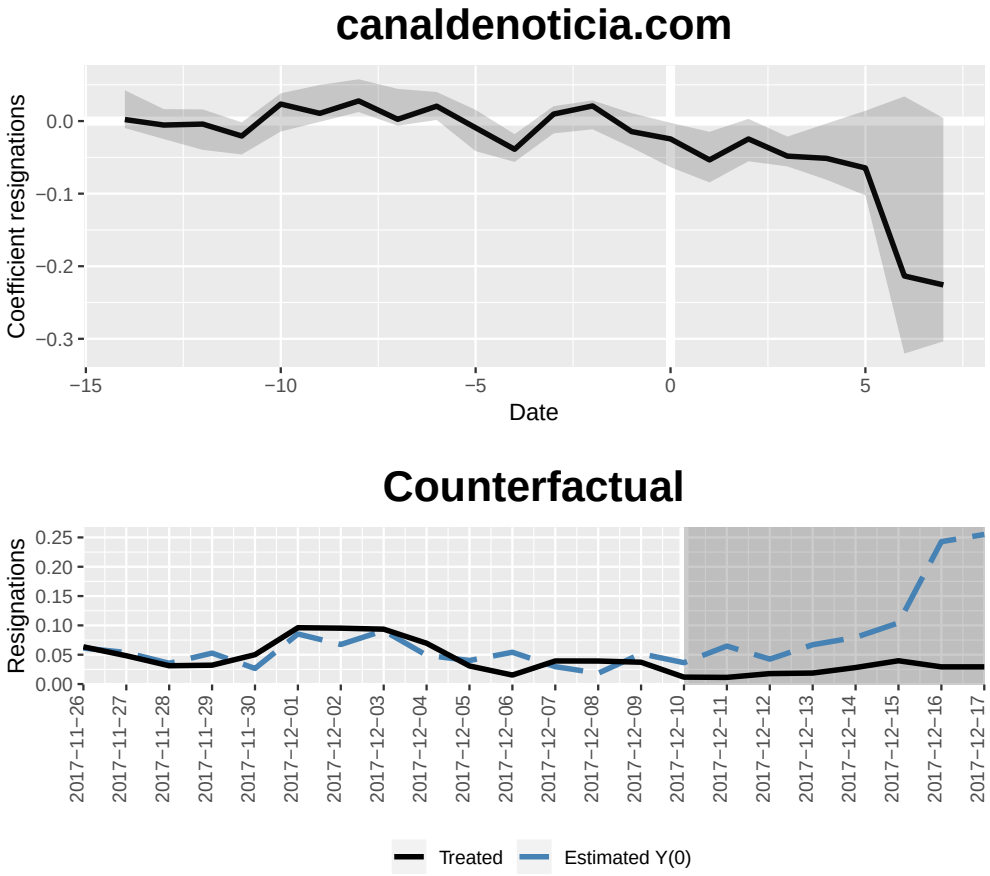

Figure D.5.7: Synthetic control model for DoS attack on canaldenoticia.com on 2017-12-10 showing the development of the topic *resignations*.

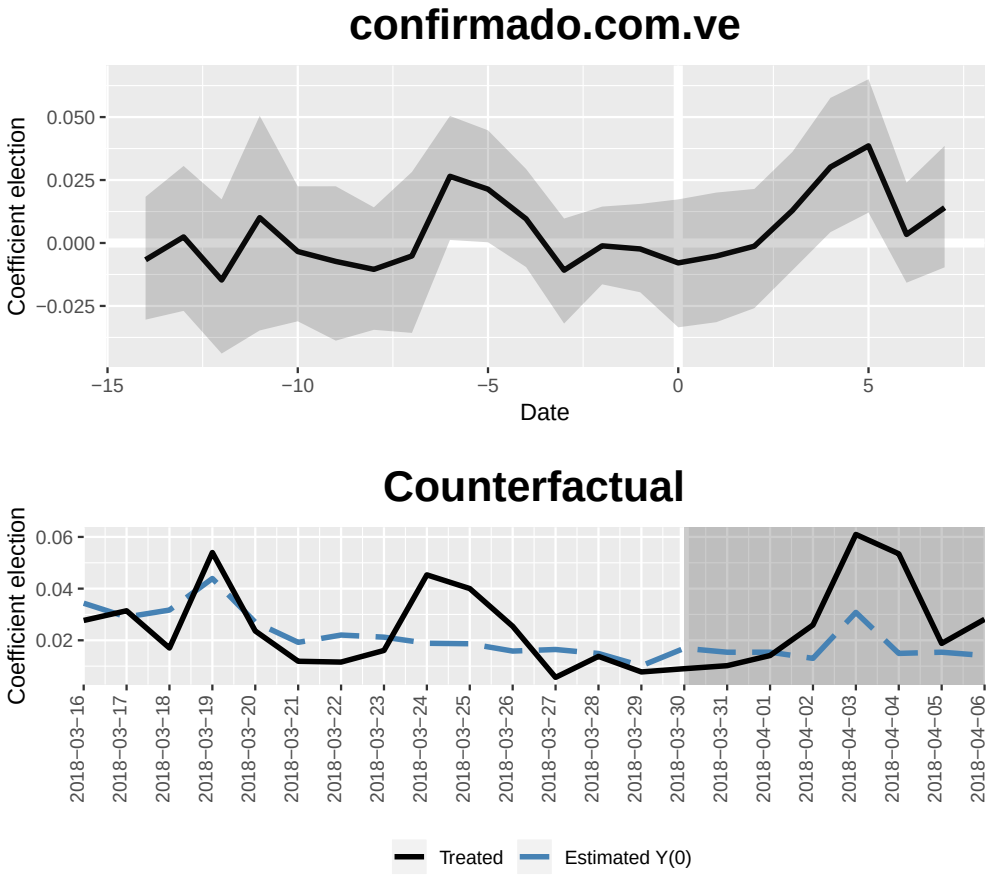

Figure D.5.8: Synthetic control model for DoS attack on confirmado.com.ve on 2018-03-30 showing the development of the topic *election*.

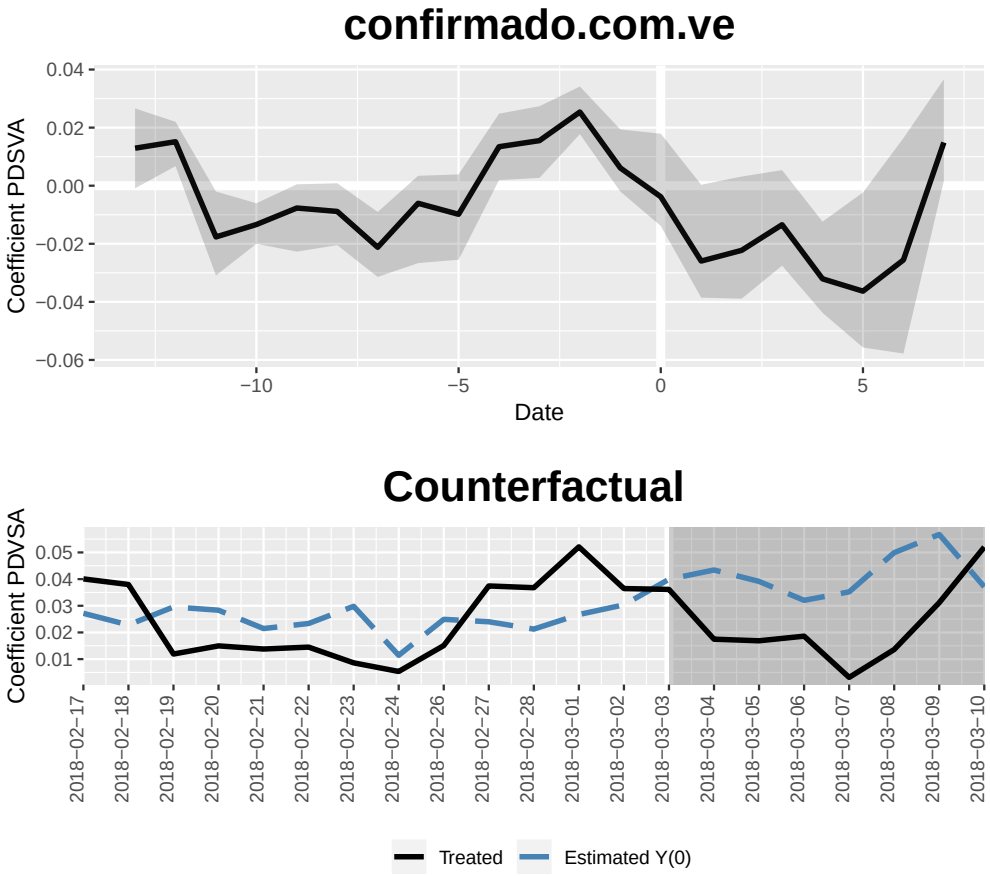

Figure D.5.9: Synthetic control model for DoS attack on confirmado.com.ve on 2018-03-03 showing the development of the topic *PDVSA*.

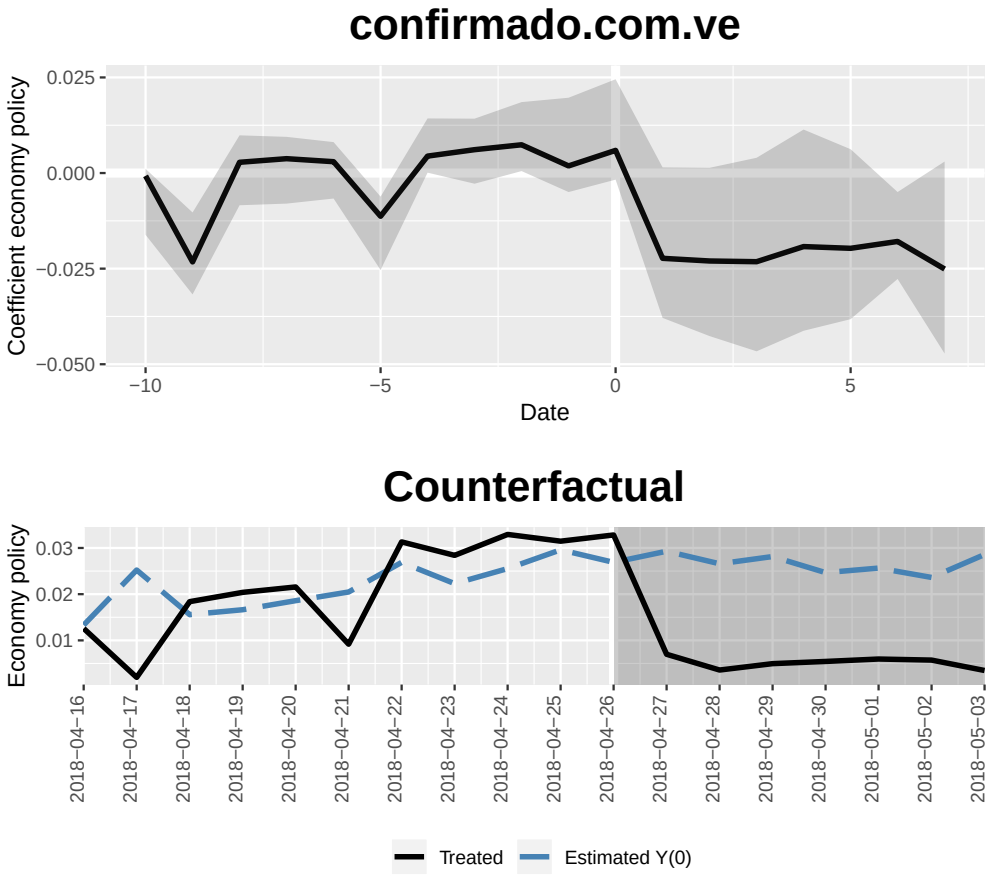

Figure D.5.10: Synthetic control model for DoS attack on confirmado.com.ve on 2018-04-26 showing the development of the topic *economy policy*.

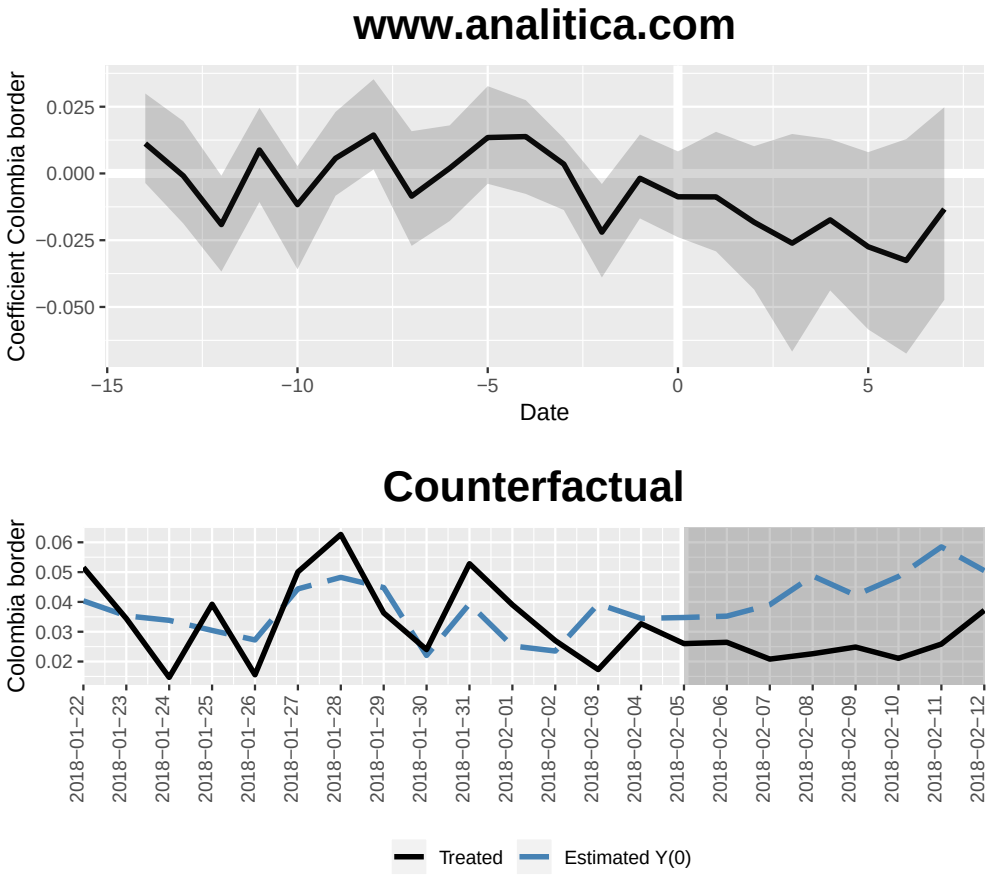

Figure D.5.11: Synthetic control model for DoS attack on www.analitica.com on 2018-02-05 showing the development of the topic *Colombia border*.

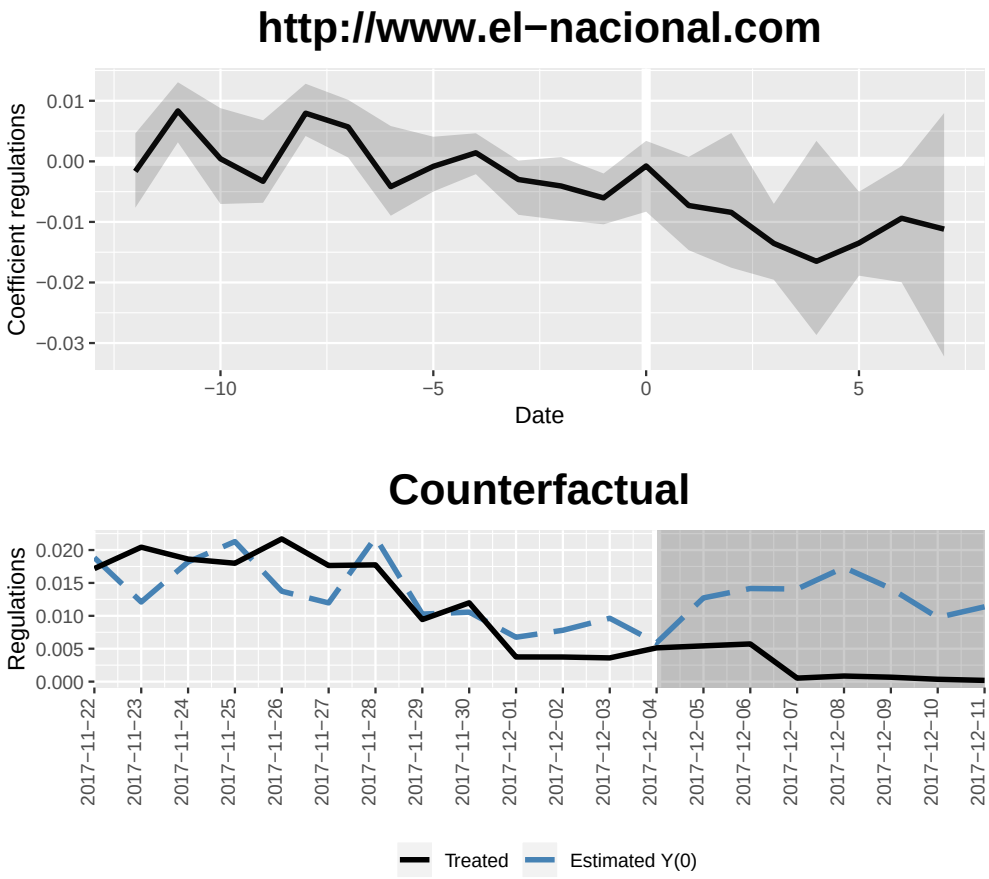

Figure D.5.12: Synthetic control model for DoS attack on el-nacional.com on 2017-12-04 showing the development of the topic *regulations*.

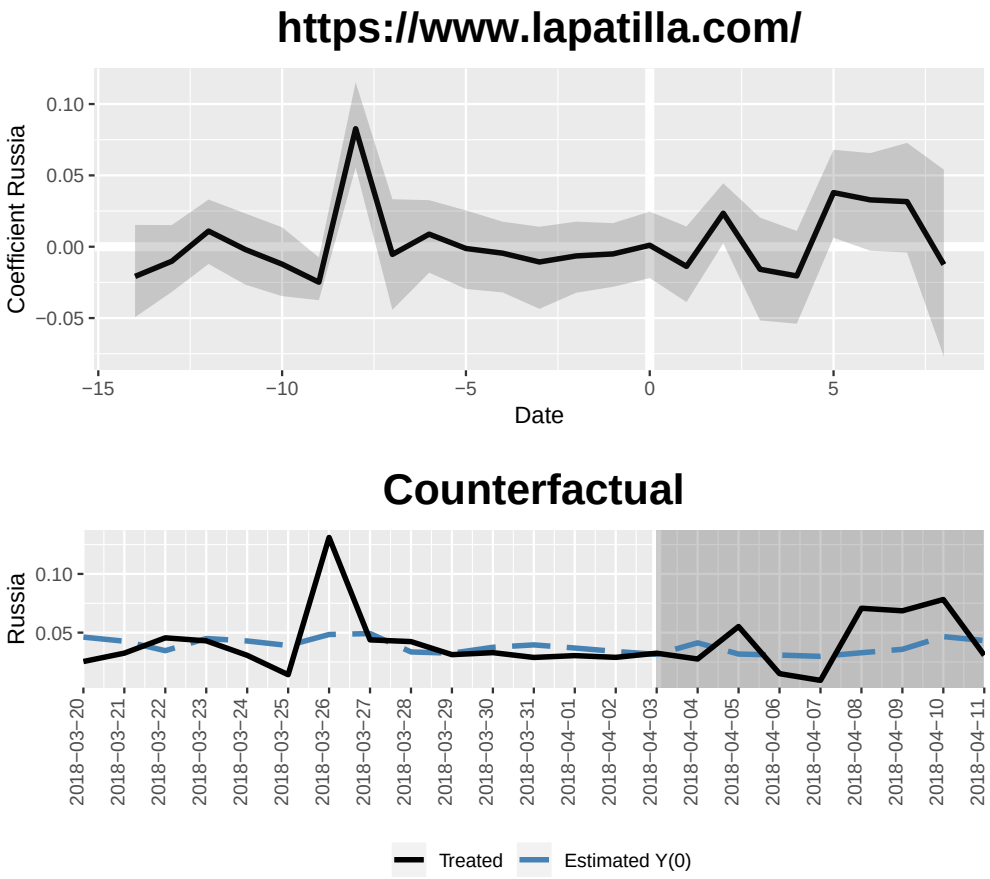

Figure D.5.13: Synthetic control model for DoS attack on lapatilla.com on 2018-04-03 showing the development of the topic *Russia*.

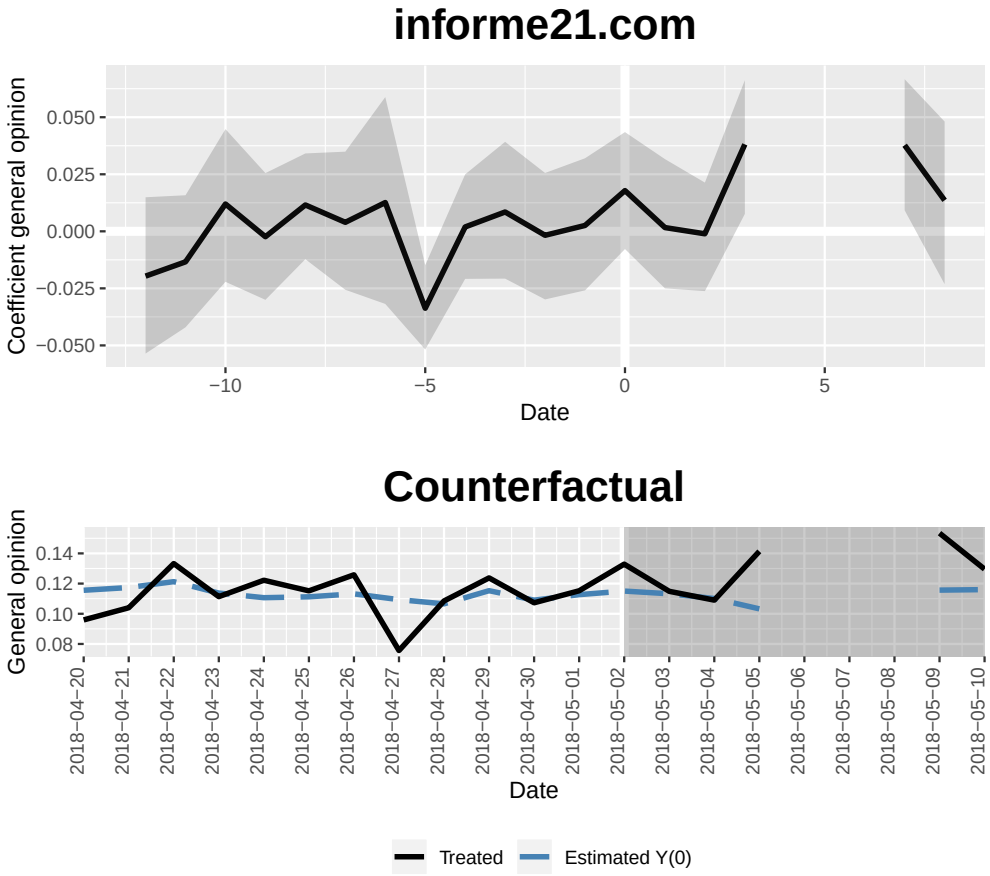

Figure D.5.14: Synthetic control model for DoS attack on informe21.com on 2018-05-02 showing the development of the topic *general opinion*.

E

Supplementary Material For Chapter 4

E.1 Sanction Threat Models and Case Study Material

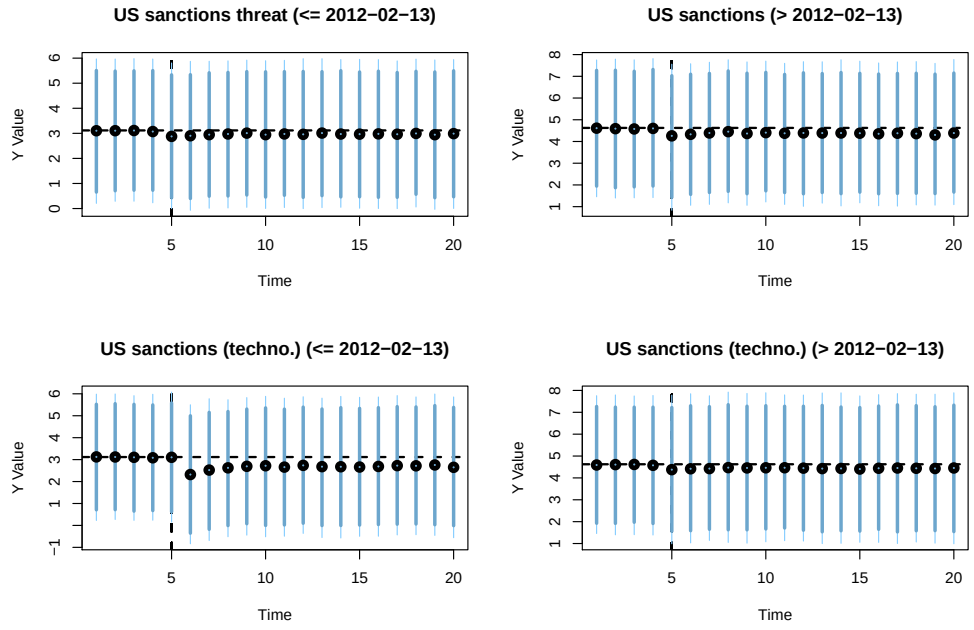

Figure E.1.1: Simulations of DoS attacks (US) - sanction threats. Note: Based on 10000 draws. 95% and 90% confidence intervals are displayed.

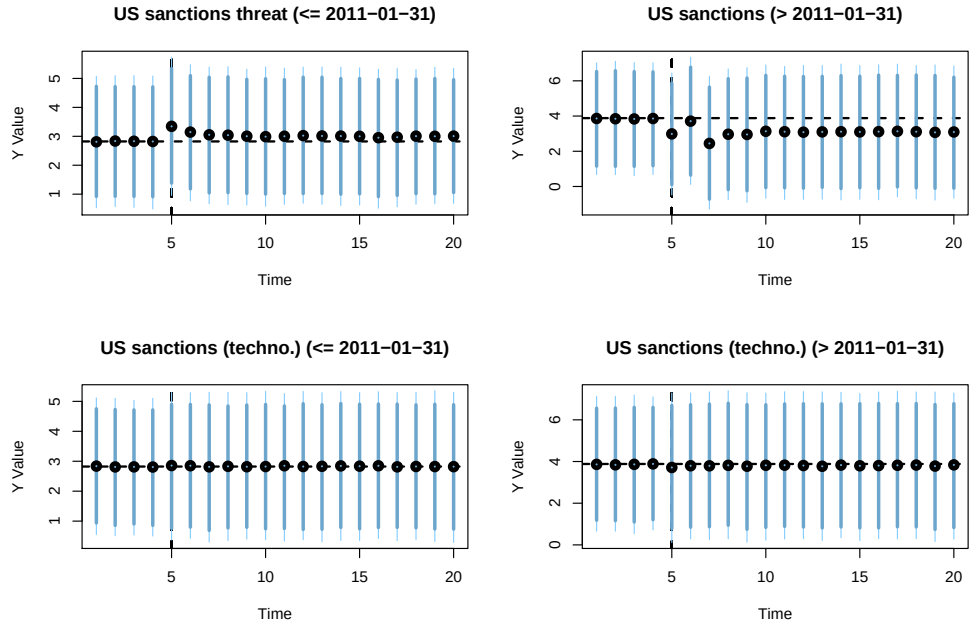

Figure E.1.2: Simulations of DoS attacks (EU) - sanction threats.

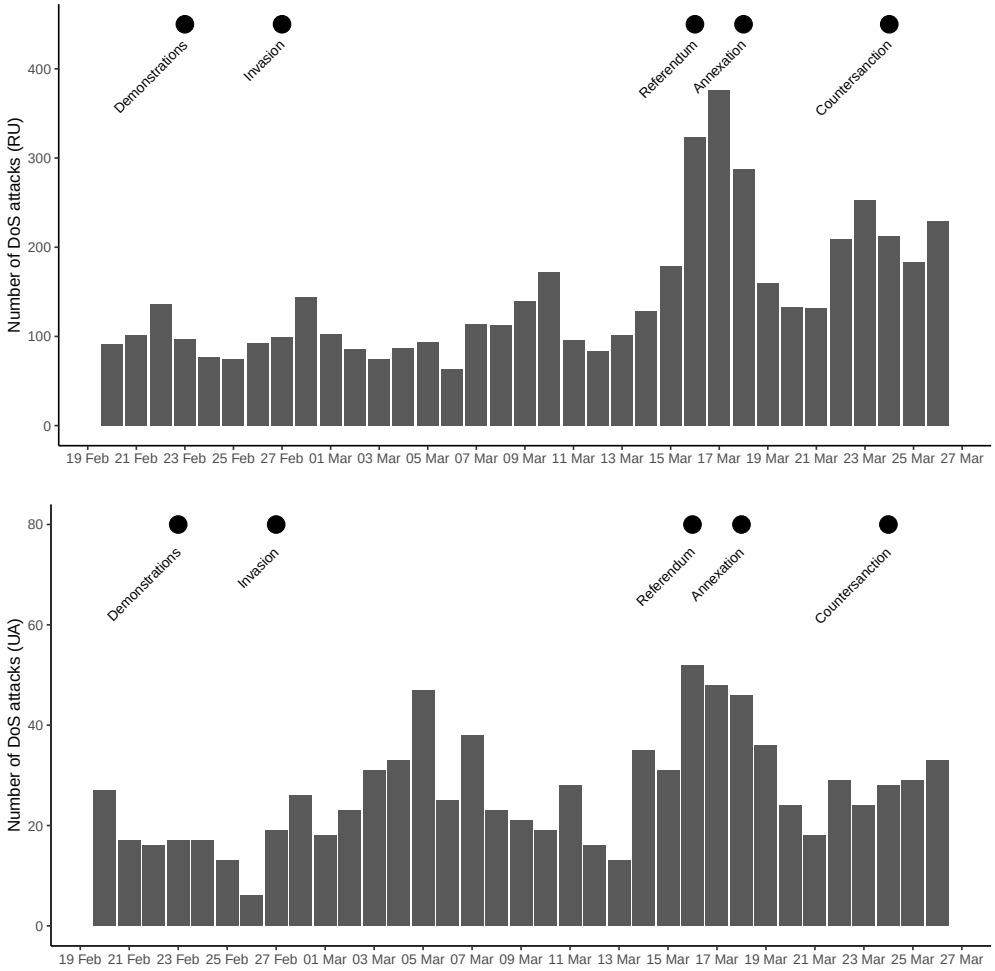

Figure E.1.3: Development of DoS attacks in Russia & Ukraine in March 2014.

	Δ DoS US <= 2012-02-13	Δ DoS US > 2012-02-13	Δ DoS US <= 2012-02-13 (techno.)	Δ DoS US > 2012-02-13 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction threat	−0.24	−0.34	−0.01	−0.23	0.54	−0.88	0.02	−0.12
	(0.41)	(0.41)	(0.49)	(0.58)	(0.34)	(0.58)	(0.48)	(0.74)
Sanction threat (t-1)			−0.77					
			(0.49)					
Δ DoS (t-1)	−0.26***	−0.21***	−0.26***	−0.21***	−0.40***	−0.38***	−0.40***	−0.38***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.21***	−0.16***	−0.21***	−0.16***	−0.34***	−0.22***	−0.34***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.18***	−0.16***	−0.18***	−0.16***	−0.23***	−0.21***	−0.23***	−0.21***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.09**	−0.00	−0.10**	−0.00	−0.23***	−0.09**	−0.23***	−0.09**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-5)	−0.05	−0.05	−0.05	−0.05	−0.16***	−0.08**	−0.16***	−0.08**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-6)	−0.07*	−0.00	−0.08**	−0.00	−0.11***	−0.10**	−0.11***	−0.10**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-7)	0.00	−0.00	0.00	−0.00	−0.09**	−0.03	−0.09**	−0.03
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-8)	−0.02	−0.00	−0.02	−0.00	−0.06	−0.00	−0.06	−0.00
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-9)	0.01	0.06*	0.01	0.06*	−0.07*	−0.03	−0.07*	−0.03
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-10)	0.02	0.01	0.02	0.01	−0.06*	−0.01	−0.07*	−0.01
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-11)	−0.05	0.05	−0.05	0.05	−0.10***	−0.04	−0.10**	−0.04
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-12)	−0.04	0.01	−0.04	0.01	−0.08**	−0.03	−0.08*	−0.03
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-13)	−0.02	−0.01	−0.02	−0.01	−0.02	0.02	−0.02	0.02
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-14)	0.06*	0.07*	0.06*	0.07*	−0.01	0.07**	−0.00	0.07**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
R^2	0.10	0.08	0.10	0.08	0.17	0.15	0.17	0.15
Adj. R^2	0.09	0.07	0.09	0.07	0.16	0.14	0.16	0.14
Num. obs.	1388	1402	1388	1402	1375	1415	1375	1415
RMSE	1.46	1.63	1.46	1.63	1.16	1.64	1.16	1.64

Table E.1.1: Threat Autoregressive Distributed Lagged (ARDL) models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

E.2 Imputation of Dependent Variable

Due to technical failures in the measurement provided by CAIDA approximately 6.9% of the observations are not available. More precisely, in these cases, the system did not post-process the internet traffic data to measure randomly spoofed DoS attacks. Nevertheless, in only three times the measurement failed for longer than ten days (with a maximum number of 52 days) and the most common failure only lasted two days. Since statistical models and simulations dealing with time series require complete time series, I imputed these missing values using ARIMA state space representation with Kalman smoothing using the R-package *imputeTS* (Moritz and Bartz-Beielstein, 2017). The best-chosen values (AR order, differencing and MA order) for the US time series were an ARIMA(5,1,3) model and for the EU time series an ARIMA(1,1,1) model with drift. Afterward, the predictions were smoothed using a Kalman algorithm (using observations before and after the NAs) due to the high volatility of the data.[1] Figure E.2.1 highlights the imputed values in red for the split time series. In general, the missing values rarely overlap with the independent variables of interest and models without the imputed values show similar results as the main models (see Table E.4.6).

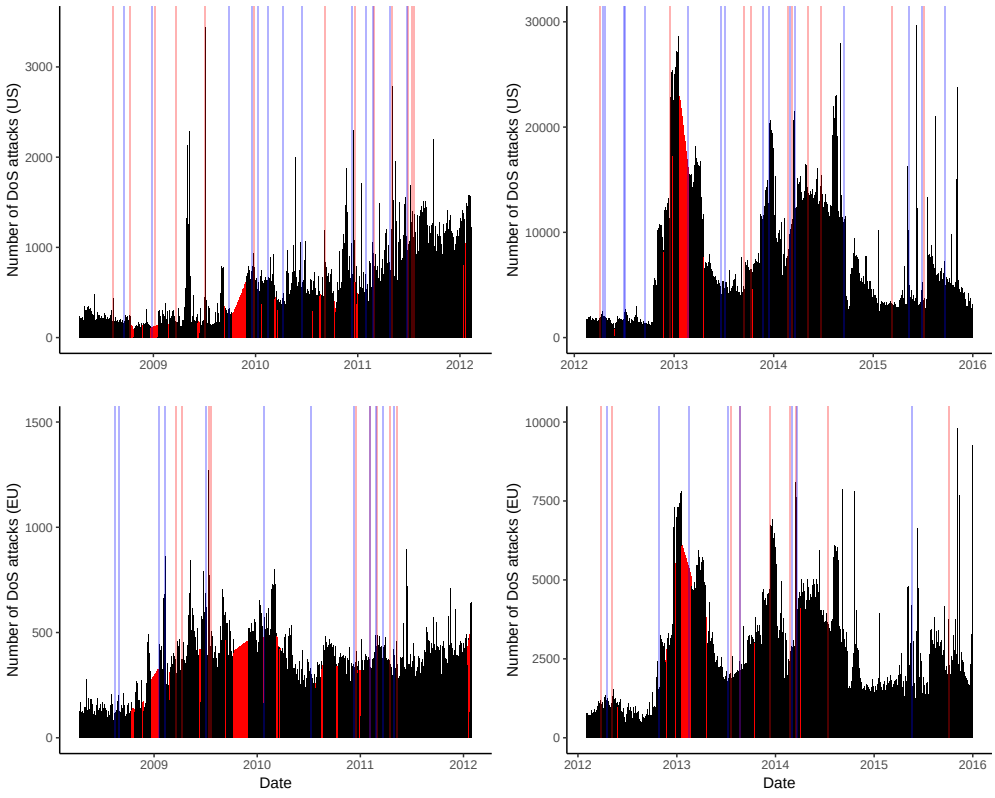

Figure E.2.1: Imputed predictions and NAs. Note: Time series split at breaking points (as calculated in Appendix E.3). Red areas indicate imputed values, while blue and red horizontal lines, the sanction threats or impositions, respectively.

[1] For more details see Gardner, Harvey and Phillips (1980).

E.3 Transformation of the Dependent Variable

First, as highlighted in the data section, the time series indicate that there could have been a structural break during the temporal development of DoS attacks. If the time series suffers from such breaks, this leads to unreliable models and estimates. To check whether this is the case, I run Pettitt tests (Pettitt, 1979; Verstraeten et al., 2006). These tests suggest indeed that there are time-breaks in both time series (see Table E.3.1 and Figures E.3.1–E.3.2). Thus, in order to run efficient time series models on the data, I divide the two time series into four with breaking points at 2012-02-13 (US time series) and 2012-01-31 (EU time series). Although it is difficult to exactly determine the reasons behind these breaks, this might have something to do with the increased use of cloud networks, content delivery networks and, in general, more internet-connected devices/servers, or simply more attacks from 2012 onward. Second, it is necessary to check for non-stationary processes within the data. A stationary process describes a stochastic process where the variance and mean of a time series do not change over time, which is a requirement for many statistical tests. Kwiatkowski-Phillips-Schmidt-Shin (KPSS) and/or Dickey-Fuller tests emphasize that all four time series suffer from non-stationary (see Table E.3.2). To solve these problems, I take the first differences of the dependent variable (Wooldridge, 2015).[2] Third, the dependent variable should be approximately normally distributed. While applied researchers find perfectly normally distributed variables only rarely, quantile-quantile plots show that the dependent variables for the US and EU and the different periods are not normally distributed and suffer from heavy tails. To counter this, I use a modified box-cox transformation that allows negative values to make the variables normally distributed (Hawkins and Weisberg, 2017). Figures E.3.3 – E.3.4 show that these transformation greatly helped in making the outcome variables normally distributed.

	U^*	p-value	Probable change point
DoS US	1953000	<0.01	2012-02-13
DoS EU	1957500	<0.01	2012-01-31

Table E.3.1: Pettitt test for structural breaks. Note: The null hypothesis, no change in the central tendency of a time series, is tested against the alternative hypothesis, change. U^* is the maximum of U, the test statistic as calculated in Verstraeten et al. (2006).

[2]For some time series the KPSS tests revealed no serious problems with non-stationary, nevertheless as the Dickey-Fuller tests suggest an unit-root, I calculate first differences also for these time series.

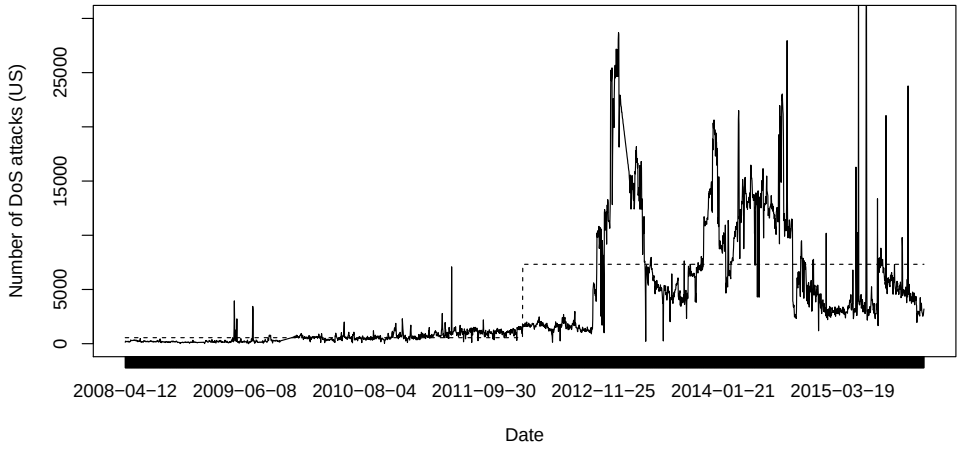

Figure E.3.1: Pettitt tests for structural breaks (US time series). Note: Outliers above 30,000 DoS attacks per day are cut-off.

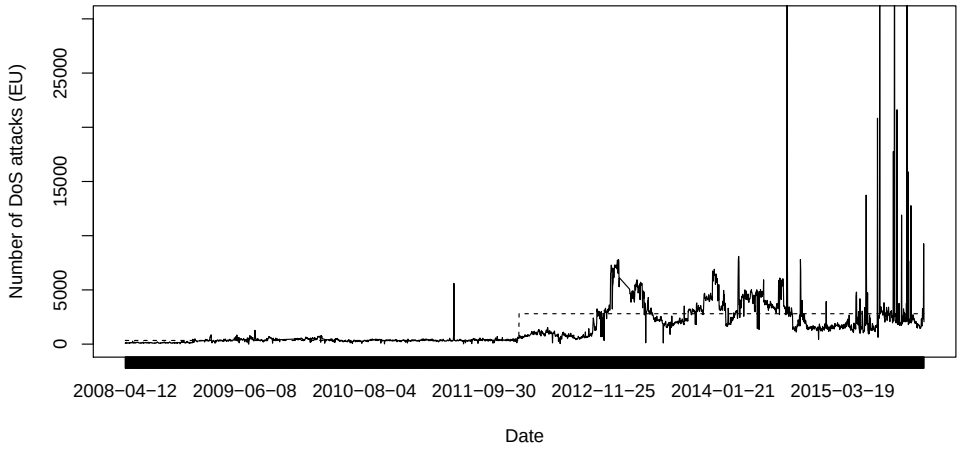

Figure E.3.2: Pettitt tests for structural breaks (EU time series). Note: Outliers above 30,000 DoS attacks per day are cut-off.

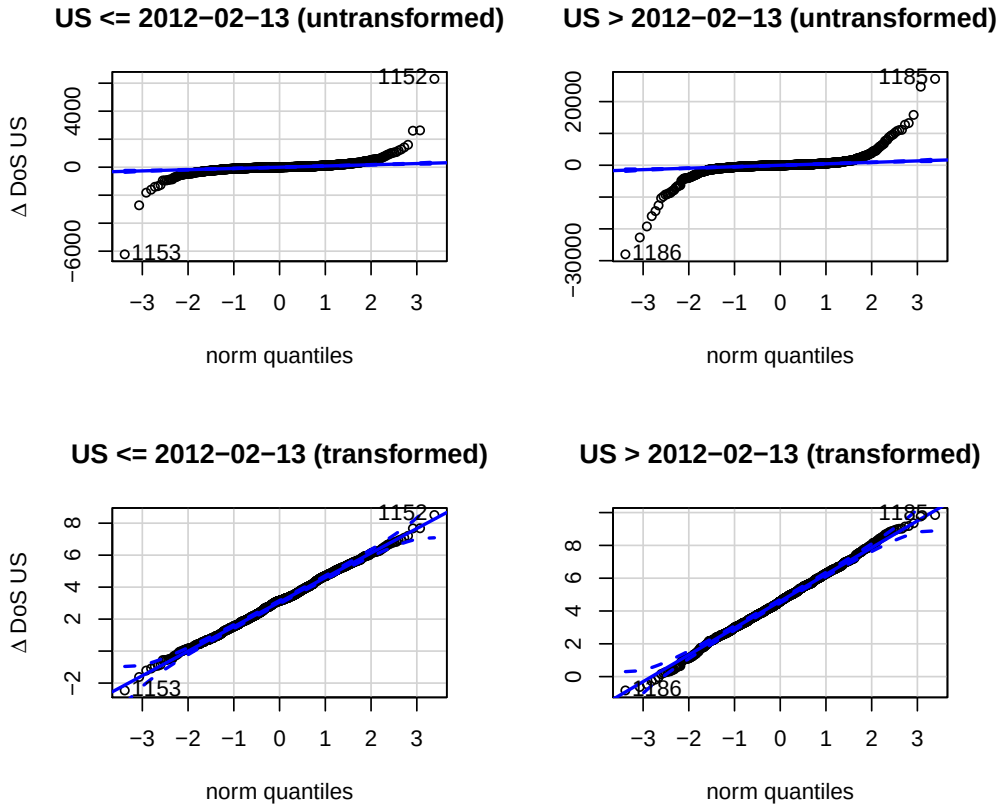

Figure E.3.3: Box-Cox transformation of Δ DoS attacks on the US.

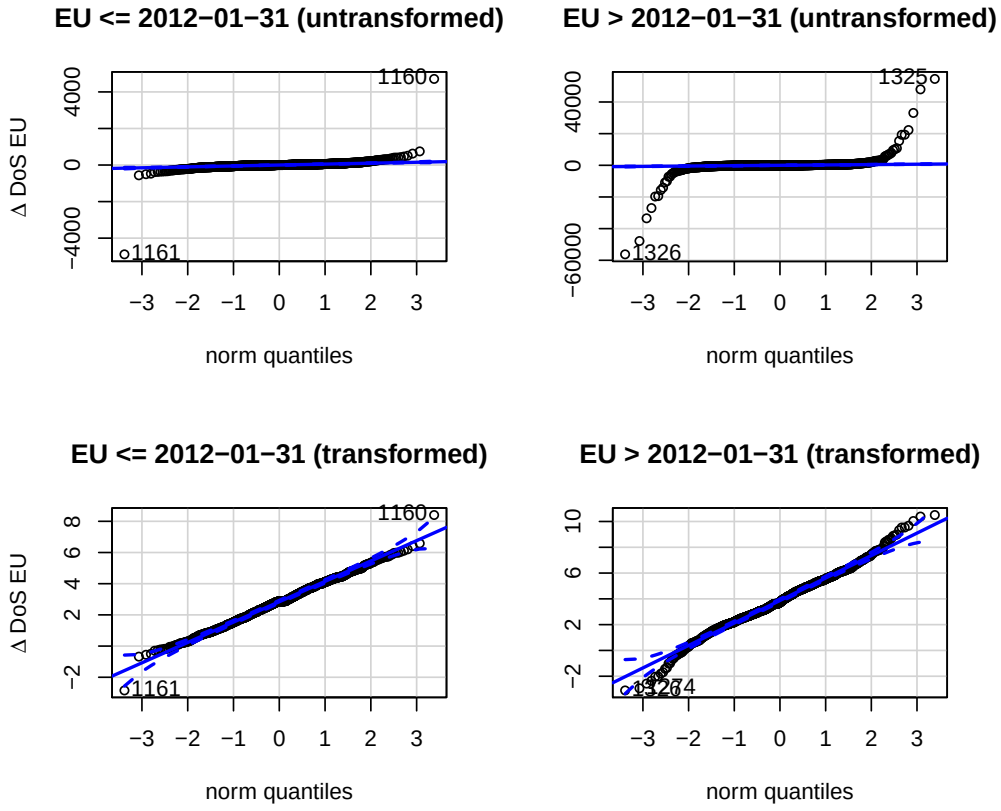

Figure E.3.4: Box-Cox transformation of Δ DoS attacks on the EU.

	KPSS test (level)	ADF test (level)	KPSS test (Δ)	ADF test (Δ)
DoS US <= 2012-02-13	<0.01	<0.01	0.10	<0.01
DoS US > 2012-02-13	0.05	0.31	0.10	<0.01
DoS EU <= 2012-01-31	0.03	<0.01	0.10	<0.01
DoS EU > 2012-01-31	0.03	<0.01	0.10	<0.01

Table E.3.2: Kwiatkowski-Phillips-Schmidt-Shin (KPSS) and Dickey-Fuller (ADF) tests for non-stationary processes. While for the ADF test the null hypothesis is the existence of a unit-root (that causes non-stationarity), the null hypothesis for the KPSS is stationarity.

E.4 Robustness and Sensitivity Tests

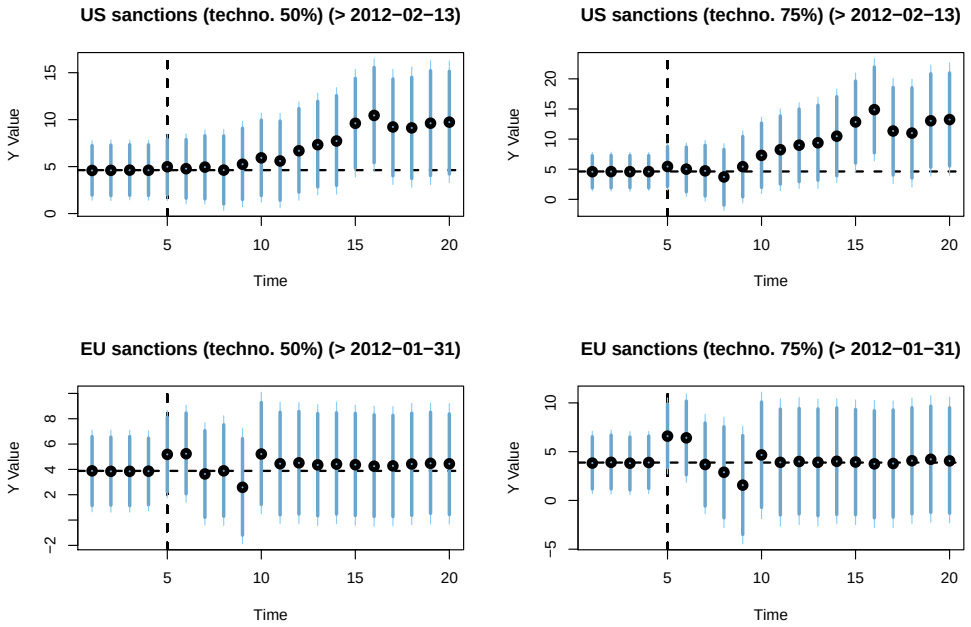

Figure E.4.1: Simulations of DoS attacks (different thresholds). Note: Based on 10000 draws. 95% and 90% confidence intervals are displayed.

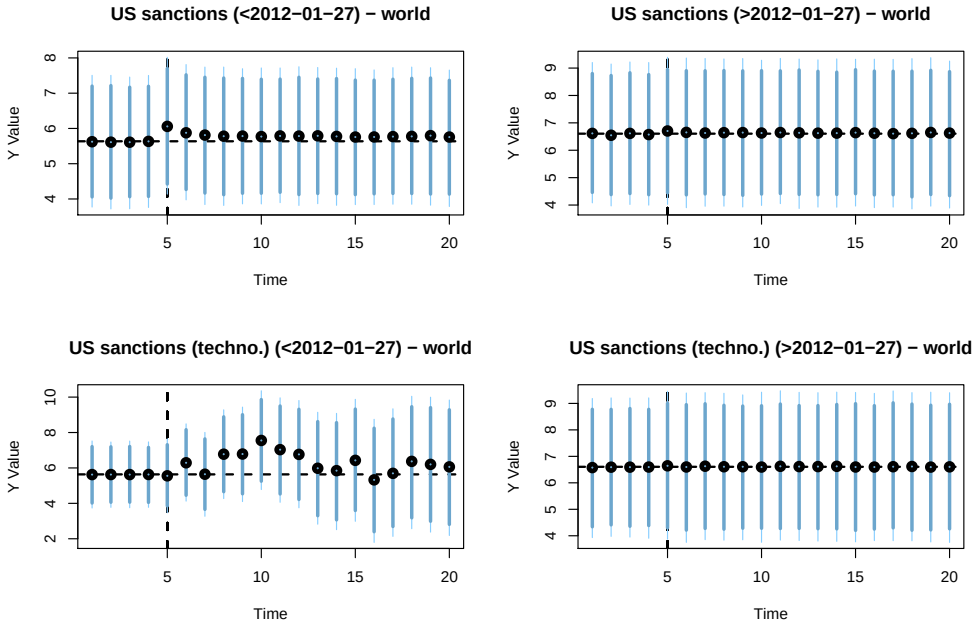

Figure E.4.2: Simulations of DoS attacks (world).

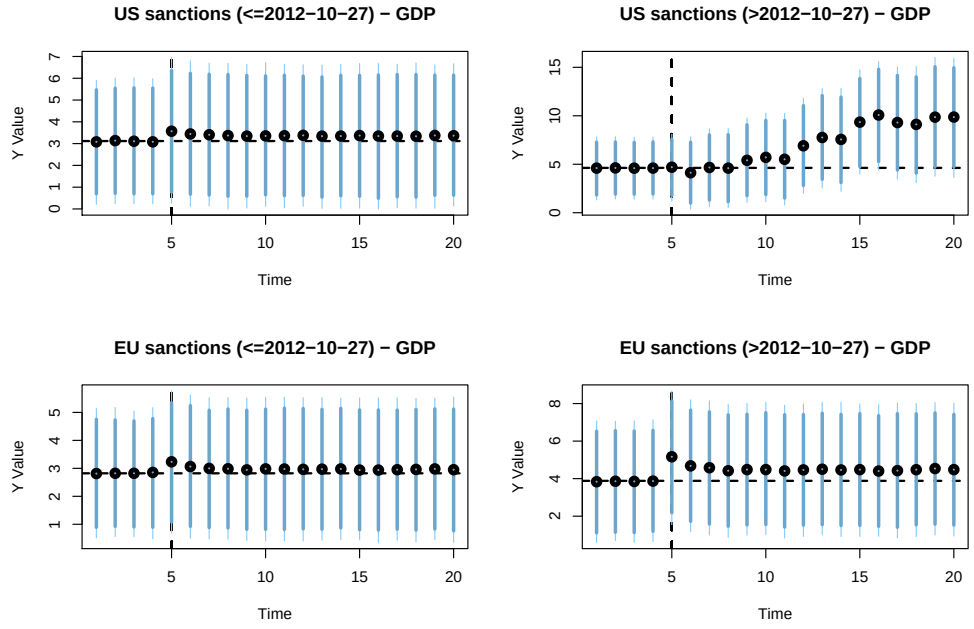

Figure E.4.3: Simulations of DoS attacks (US) - GDP.

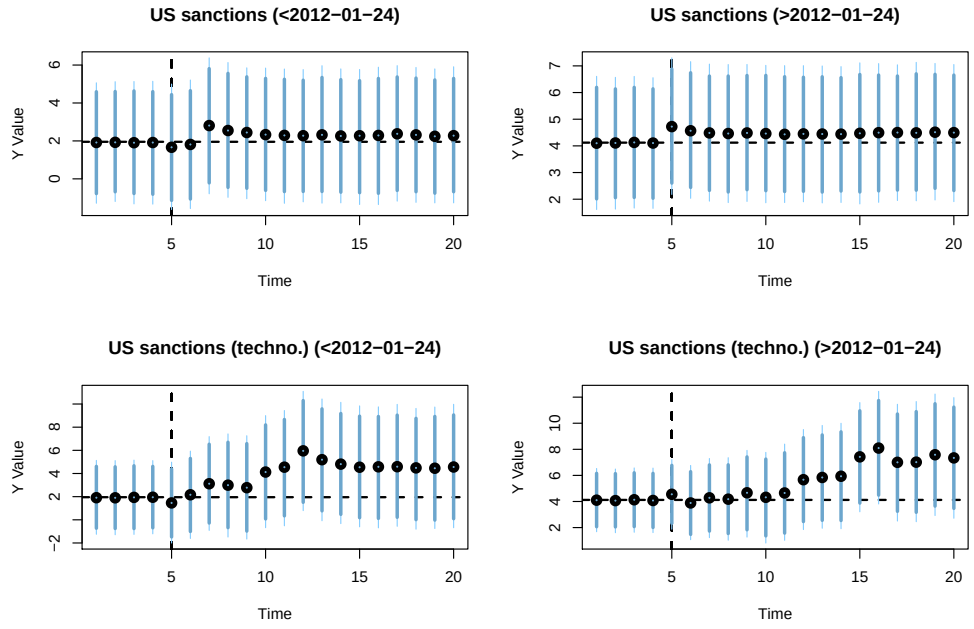

Figure E.4.4: Simulations of DoS attacks (US) - strong attacks.

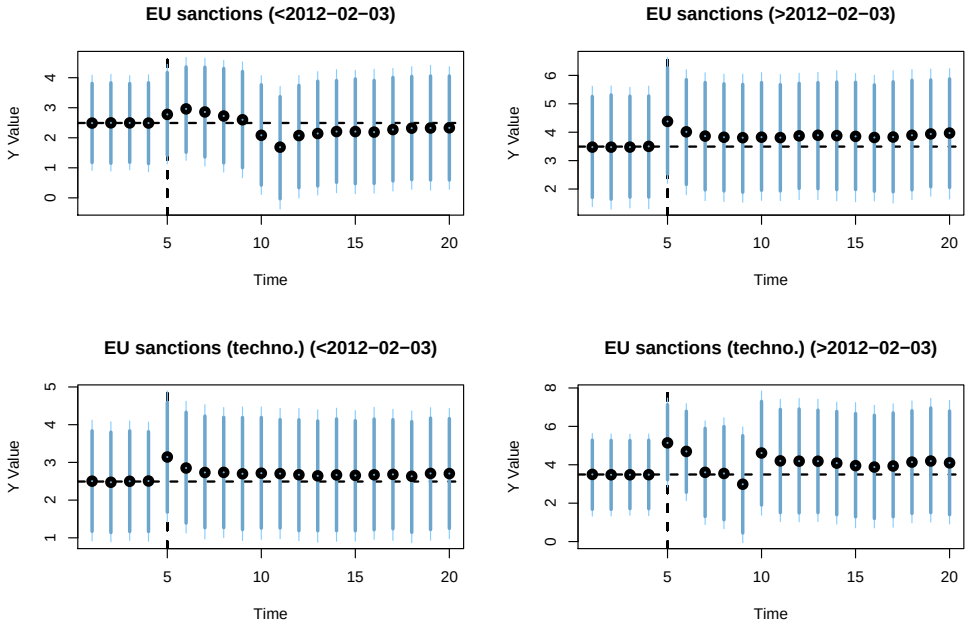

Figure E.4.5: Simulations of DoS attacks (EU) - strong attacks.

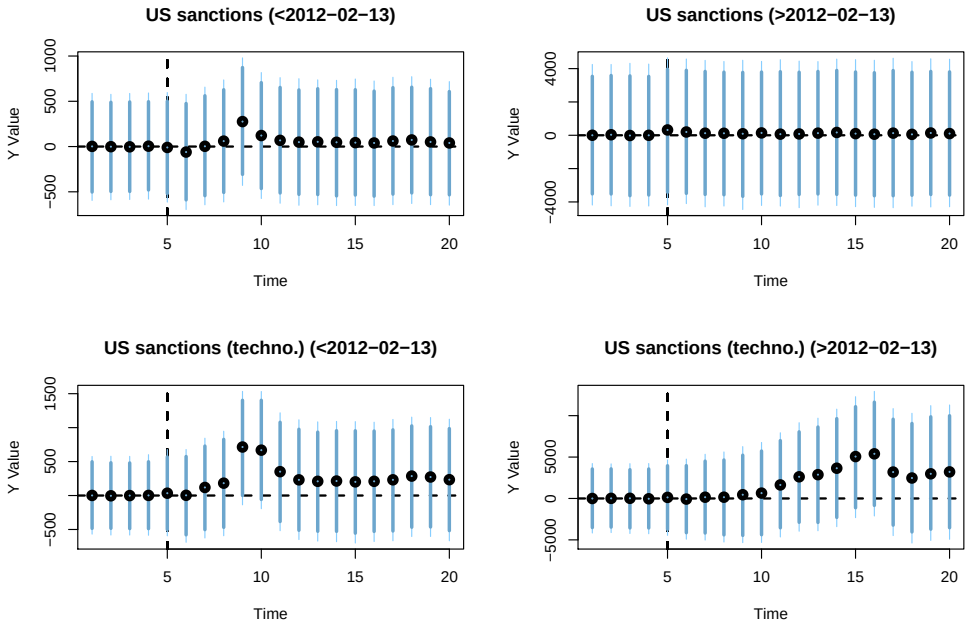

Figure E.4.6: Simulations of DoS attacks (US) - untransformed.

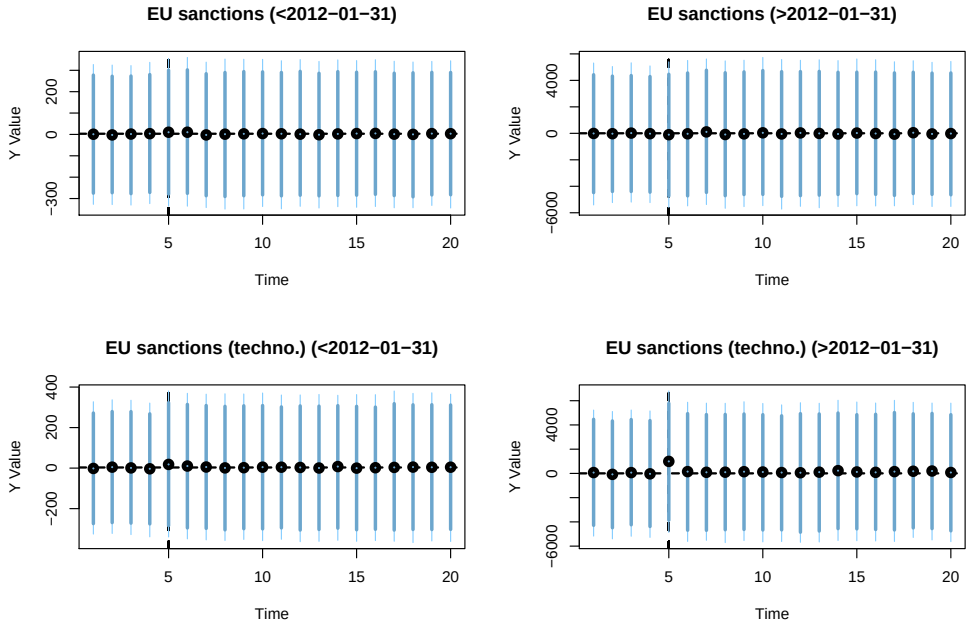

Figure E.4.7: Simulations of DoS attacks (EU) - untransformed.

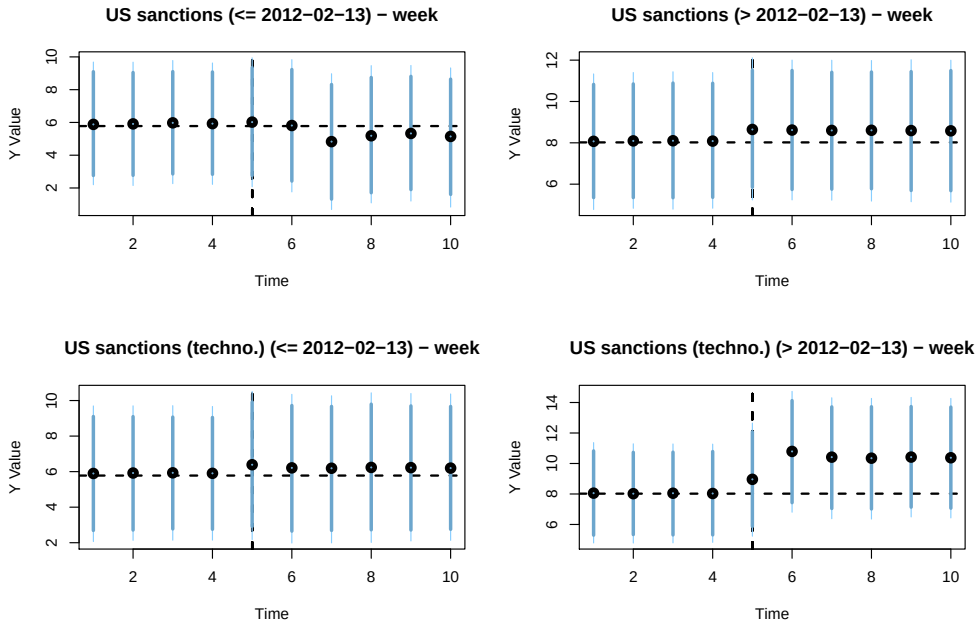

Figure E.4.8: Simulations of DoS attacks (US) - week level.

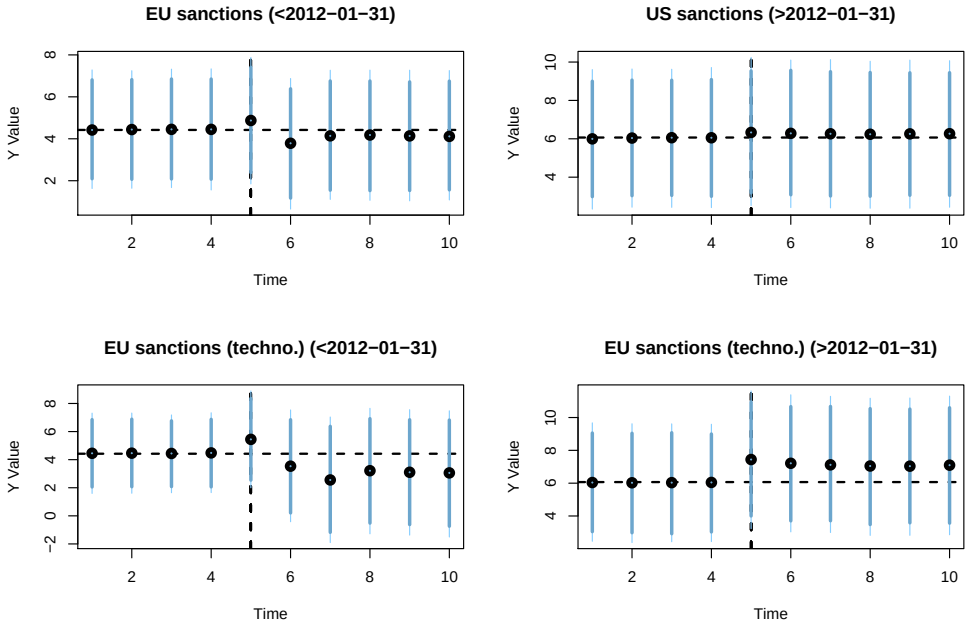

Figure E.4.9: Simulations of DoS attacks (EU) - week level.

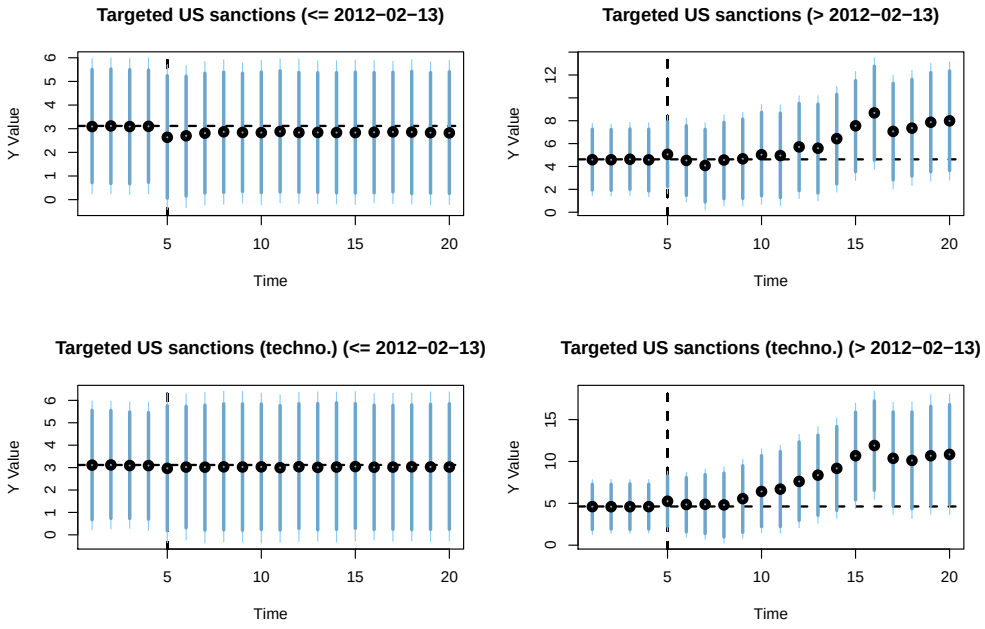

Figure E.4.10: Simulations of DoS attacks (US) - Targeted sanctions.

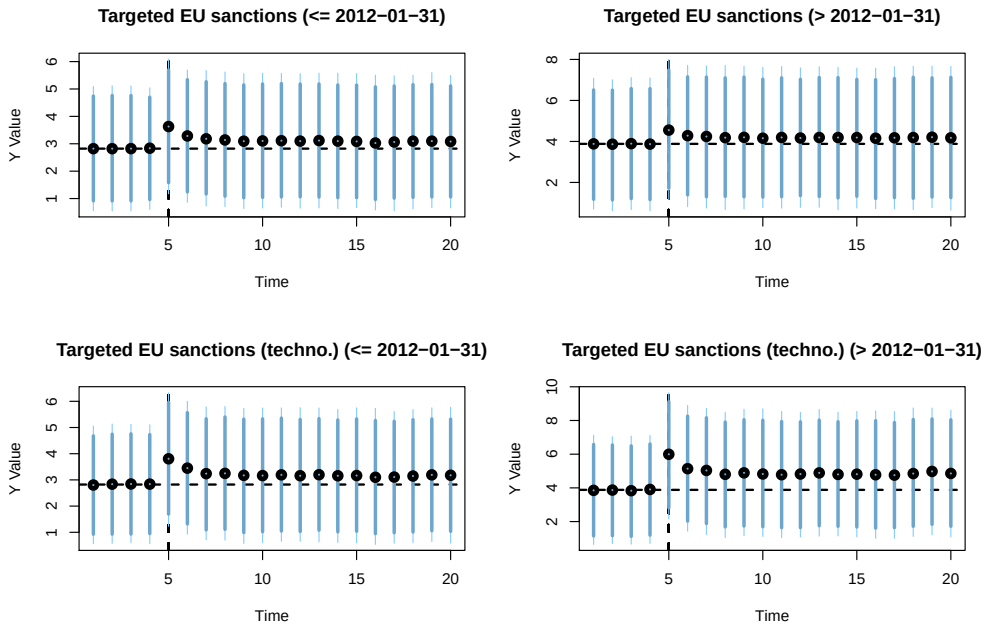

Figure E.4.11: Simulations of DoS attacks (EU) - Targeted sanctions.

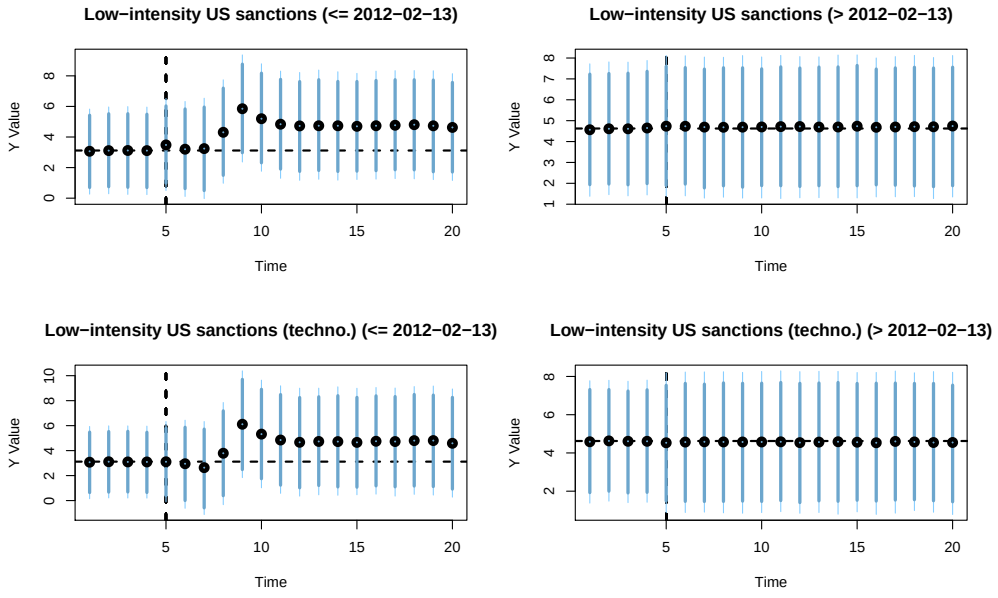

Figure E.4.12: Simulations of DoS attacks (US) - Low-intensity sanctions.

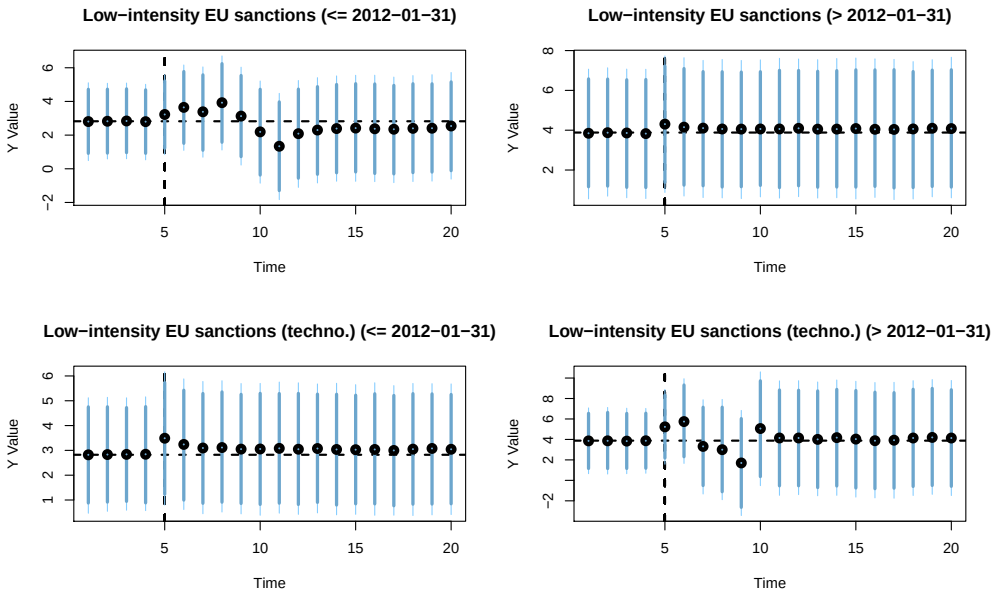

Figure E.4.13: Simulations of DoS attacks (EU) - Low-intensity sanctions.

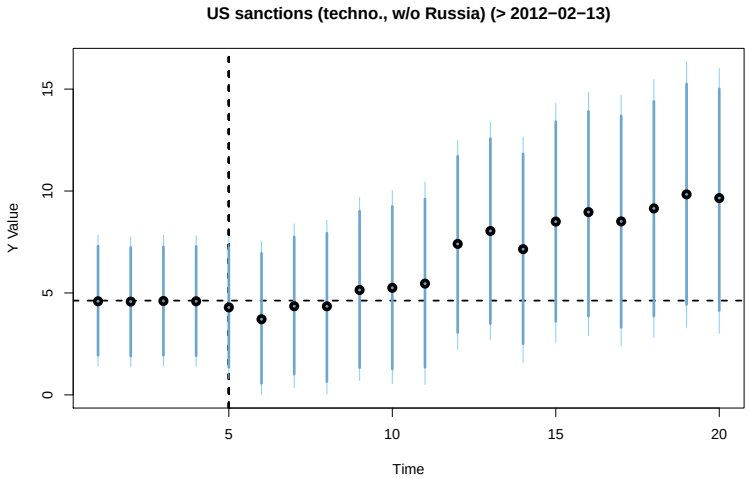

Figure E.4.14: Simulations of DoS attacks (US) - Sanctions on techno. countries (without Russia).

	Δ DoS US > 2012-02-13 (techno., 50%)	Δ DoS US > 2012-02-13 (techno., 75%)	Δ DoS EU > 2012-01-31 (techno., 50%)	Δ DoS EU > 2012-01-31 (techno., 75%)
Sanction (t-1)	−0.12	−0.30	0.56	0.87
	(0.73)	(1.15)	(0.74)	(1.16)
Sanction (t-2)	0.15	−0.24	−1.27	−2.21
	(0.73)	(1.15)	(0.74)	(1.16)
Sanction (t-3)	−0.25	−0.98	−0.11	−1.33
	(0.73)	(1.15)	(0.74)	(1.16)
Sanction (t-4)	0.62	1.37	−1.42	−2.06
	(0.73)	(1.15)	(0.74)	(1.16)
Sanction (t-5)	0.78	2.01	1.97**	2.11
	(0.73)	(1.15)	(0.74)	(1.16)
Sanction (t-6)	−0.16	1.44		
	(0.73)	(1.15)		
Sanction (t-7)	1.21	1.53		
	(0.73)	(1.15)		
Sanction (t-8)	0.97	0.98		
	(0.73)	(1.15)		
Sanction (t-9)	0.63	1.49		
	(0.74)	(1.15)		
Sanction (t-10)	2.22**	2.73*		
	(0.73)	(1.15)		
Sanction (t-11)	1.39	2.78*		
	(0.73)	(1.15)		
Sanction (t-12)	−0.68	−2.52*		
	(0.73)	(1.15)		
Sanction (t-13)	0.06	−0.42		
	(0.73)	(1.15)		
Sanction (t-14)	0.46	1.75		
	(0.73)	(1.15)		
Sanction threat	−0.48	1.39	−0.11	−0.24
	(0.68)	(1.15)	(0.73)	(0.82)
Δ DoS (t-1)	−0.21***	−0.22***	−0.38***	−0.39***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.16***	−0.15***	−0.22***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.16***	−0.16***	−0.21***	−0.20***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)			−0.09**	−0.08**
			(0.03)	(0.03)
Δ DoS (t-5)			−0.08**	−0.08**
			(0.03)	(0.03)
Δ DoS (t-6)			−0.10**	−0.10**
			(0.03)	(0.03)
Δ DoS (t-7)			−0.04	−0.04
			(0.03)	(0.03)
Δ DoS (t-8)			−0.00	−0.01
			(0.03)	(0.03)
Δ DoS (t-9)			−0.04	−0.03
			(0.03)	(0.03)
Δ DoS (t-10)			−0.01	−0.02
			(0.03)	(0.03)
Δ DoS (t-11)			−0.04	−0.04
			(0.03)	(0.03)
Δ DoS (t-12)			−0.03	−0.03
			(0.03)	(0.03)
Δ DoS (t-13)			0.02	0.02
			(0.03)	(0.03)
Δ DoS (t-14)			0.07**	0.08**
			(0.03)	(0.03)
R^2	0.08	0.09	0.16	0.16
Adj. R^2	0.07	0.07	0.15	0.15
Num. obs.	1402	1402	1415	1415
RMSE	1.63	1.62	1.64	1.64

Table E.4.1: Different Thresholds ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS (world) <= 2012-01-27	Δ DoS (world) > 2012-01-27	Δ DoS (world) <= 2012-01-27 (techno.)	Δ DoS (world) > 2012-01-27 (techno.)
Sanction	0.41	0.08	−0.05	0.06
	(0.26)	(0.37)	(0.43)	(0.54)
Sanction (t-1)			0.70	
			(0.43)	
Sanction (t-2)			−0.41	
			(0.43)	
Sanction (t-3)			1.14**	
			(0.43)	
Sanction (t-4)			0.37	
			(0.43)	
Sanction (t-5)			1.11**	
			(0.43)	
Sanction (t-6)			−0.02	
			(0.43)	
Sanction (t-7)			−0.02	
			(0.43)	
Sanction (t-8)			−0.78	
			(0.43)	
Sanction (t-9)			−0.42	
			(0.43)	
Sanction (t-10)			0.24	
			(0.43)	
Sanction (t-11)			−1.20**	
			(0.43)	
Sanction (t-12)			−0.04	
			(0.43)	
Sanction (t-13)			0.41	
			(0.43)	
Sanction (t-14)			−0.05	
			(0.43)	
Sanction threat	0.19	−0.08	−0.03	−0.02
	(0.27)	(0.35)	(0.32)	(0.47)
Sanction threat (t-1)			−0.53	
			(0.32)	
Δ DoS (t-1)	−0.36***	−0.30***	−0.36***	−0.30***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.34***	−0.20***	−0.34***	−0.20***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.24***	−0.21***	−0.23***	−0.21***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.17***	−0.08**	−0.16***	−0.09**
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-5)	−0.15***	−0.09**	−0.13***	−0.10***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-6)	−0.10**	−0.06*	−0.08**	−0.07*
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-7)	−0.04	−0.06*		−0.06*
	(0.03)	(0.03)		(0.03)
Δ DoS (t-8)	−0.02	−0.03		−0.03
	(0.03)	(0.03)		(0.03)
Δ DoS (t-9)	−0.07*	−0.06*		−0.06*
	(0.03)	(0.03)		(0.03)
Δ DoS (t-10)	−0.07*	−0.03		−0.04
	(0.03)	(0.03)		(0.03)
Δ DoS (t-11)	−0.07*	−0.05		−0.05
	(0.03)	(0.03)		(0.03)
Δ DoS (t-12)	−0.05	−0.04		−0.04
	(0.03)	(0.03)		(0.03)
Δ DoS (t-13)	−0.03	−0.01		−0.01
	(0.03)	(0.03)		(0.03)
Δ DoS (t-14)	0.01	0.04		0.04
	(0.03)	(0.03)		(0.03)
R^2	0.16	0.12	0.17	0.11
Adj. R^2	0.15	0.11	0.16	0.10
Num. obs.	1396	1394	1396	1394
RMSE	0.96	1.32	0.95	1.32

Table E.4.2: World ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-01-31 (GDP)	Δ DoS US > 2012-01-31 (GDP)	Δ DoS EU <= 2012-01-31 (GDP)	Δ DoS EU > 2012-01-31 (GDP)
Sanction	0.51	0.09	0.42	1.31
	(0.85)	(0.66)	(0.60)	(0.73)
Sanction (t-1)		−0.55		0.56
		(0.66)		(0.74)
Sanction (t-2)		0.44		−1.27
		(0.66)		(0.74)
Sanction (t-3)		−0.03		−0.11
		(0.66)		(0.74)
Sanction (t-4)		0.79		−1.42
		(0.66)		(0.74)
Sanction (t-5)		0.57		1.97**
		(0.66)		(0.74)
Sanction (t-6)		−0.02		
		(0.66)		
Sanction (t-7)		1.53*		
		(0.66)		
Sanction (t-8)		1.18		
		(0.67)		
Sanction (t-9)		0.21		
		(0.69)		
Sanction (t-10)		2.07**		
		(0.67)		
Sanction (t-11)		1.23		
		(0.67)		
Sanction (t-12)		−0.35		
		(0.67)		
Sanction (t-13)		0.07		
		(0.67)		
Sanction (t-14)		0.69		
		(0.66)		
Sanction threat	−0.08	0.17	−0.07	−0.11
	(0.60)	(0.53)	(0.54)	(0.73)
Δ DoS (t-1)	−0.26***	−0.21***	−0.40***	−0.38***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.21***	−0.16***	−0.33***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.18***	−0.16***	−0.23***	−0.21***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.09**		−0.23***	−0.09**
	(0.03)		(0.03)	(0.03)
Δ DoS (t-5)	−0.05		−0.16***	−0.08**
	(0.03)		(0.03)	(0.03)
Δ DoS (t-6)	−0.07*		−0.11***	−0.10**
	(0.03)		(0.03)	(0.03)
Δ DoS (t-7)	0.00		−0.09**	−0.04
	(0.03)		(0.03)	(0.03)
Δ DoS (t-8)	−0.02		−0.06	−0.00
	(0.03)		(0.03)	(0.03)
Δ DoS (t-9)	0.01		−0.07*	−0.04
	(0.03)		(0.03)	(0.03)
Δ DoS (t-10)	0.03		−0.07*	−0.01
	(0.03)		(0.03)	(0.03)
Δ DoS (t-11)	−0.05		−0.10**	−0.04
	(0.03)		(0.03)	(0.03)
Δ DoS (t-12)	−0.04		−0.08*	−0.03
	(0.03)		(0.03)	(0.03)
Δ DoS (t-13)	−0.02		−0.02	0.02
	(0.03)		(0.03)	(0.03)
Δ DoS (t-14)	0.06*		−0.00	0.07**
	(0.03)		(0.03)	(0.03)
R^2	0.10	0.08	0.17	0.16
Adj. R^2	0.09	0.07	0.16	0.15
Num. obs.	1388	1402	1375	1415
RMSE	1.46	1.62	1.16	1.64

Table E.4.3: GDP ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-01-24	Δ DoS US > 2012-01-24	Δ DoS US <= 2012-01-24 (techno.)	Δ DoS US > 2012-01-24 (techno.)	Δ DoS EU <= 2012-02-03	Δ DoS EU > 2012-02-03	Δ DoS EU <= 2012-02-03 (techno.)	Δ DoS EU > 2012-02-03 (techno.)
Sanction	−0.28	0.62	−0.48	0.43	0.28	0.90*	0.67	1.67***
	(0.44)	(0.35)	(0.74)	(0.51)	(0.25)	(0.36)	(0.38)	(0.49)
Sanction (t-1)	0.09		0.61	−0.53	0.34			0.26
	(0.44)		(0.74)	(0.51)	(0.25)			(0.49)
Sanction (t-2)	0.98*		1.05	0.28	0.08			−0.75
	(0.44)		(0.73)	(0.51)	(0.25)			(0.49)
Sanction (t-3)			0.20	−0.02	−0.04			−0.23
			(0.74)	(0.51)	(0.25)			(0.49)
Sanction (t-4)			0.00	0.45	−0.12			−0.75
			(0.74)	(0.51)	(0.25)			(0.49)
Sanction (t-5)			1.48*	−0.18				1.26*
			(0.73)	(0.51)				(0.49)
Sanction (t-6)			0.83	0.29				
			(0.74)	(0.51)				
Sanction (t-7)			1.88*	1.14*				
			(0.74)	(0.51)				
Sanction (t-8)				0.49				
				(0.52)				
Sanction (t-9)				0.39				
				(0.52)				
Sanction (t-10)				1.74***				
				(0.52)				
Sanction (t-11)				1.22*				
				(0.52)				
Sanction (t-12)				−0.49				
				(0.52)				
Sanction (t-13)				0.10				
				(0.52)				
Sanction (t-14)				0.63				
				(0.52)				
Sanction threat		−0.42	0.05	−0.09	0.07	−0.22	−0.47	0.28
		(0.33)	(0.55)	(0.45)	(0.24)	(0.39)	(0.34)	(0.49)
Δ DoS (t-1)	−0.27***	−0.28***	−0.27***	−0.29***	−0.48***	−0.43***	−0.46***	−0.43***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.19***	−0.19***	−0.20***	−0.20***	−0.38***	−0.32***	−0.37***	−0.32***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.19***	−0.12***	−0.20***	−0.13***	−0.27***	−0.25***	−0.27***	−0.25***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.12***	−0.04	−0.12***	−0.05	−0.24***	−0.18***	−0.24***	−0.18***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-5)	−0.10***	−0.08**	−0.11***	−0.08**	−0.14***	−0.14***	−0.14***	−0.14***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-6)	−0.06*	−0.05	−0.06*	−0.06*	−0.13***	−0.10**	−0.14***	−0.10**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-7)	−0.07*	−0.03	−0.06*	−0.04	−0.17***	−0.02	−0.16***	−0.02
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-8)	−0.06*	−0.04	−0.06*	−0.05	−0.18***	0.03	−0.17***	0.03
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-9)	−0.00	0.02	0.00		−0.11***	0.00	−0.11**	−0.01
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-10)	0.03	0.02	0.03		−0.13***	−0.00	−0.12***	−0.02
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-11)	−0.01	0.04	−0.01		−0.09**	−0.02	−0.08*	−0.05
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-12)	−0.06*	0.04	−0.06*		−0.08*	−0.02	−0.08*	−0.06*
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-13)	−0.01	0.01	−0.00		−0.08**	0.06	−0.08**	0.01
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-14)	0.02	0.05	0.02		−0.02	0.09**	−0.02	0.03
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-15)						0.12***		
						(0.03)		
R^2	0.10	0.10	0.11	0.11	0.22	0.20	0.22	0.19
Adj. R^2	0.09	0.09	0.09	0.09	0.20	0.18	0.20	0.18
Num. obs.	1368	1422	1368	1422	1378	1410	1378	1412
RMSE	1.63	1.26	1.63	1.26	0.80	1.08	0.80	1.09

Table E.4.4: Strong Attack ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-01-31	Δ DoS US > 2012-01-31	Δ DoS US <= 2012-01-31 (techno.)	Δ DoS US > 2012-01-31 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction	−3.65	322.21	−0.48	131.89	15.45	−118.87	22.42	981.83
	(80.85)	(600.08)	(0.74)	(879.88)	(51.54)	(908.51)	(76.56)	(1196.22)
Sanction (t-1)	−62.63		0.61	−191.29				
	(80.67)		(0.74)	(879.85)				
Sanction (t-2)	35.69		1.05	194.64				
	(80.68)		(0.73)	(879.75)				
Sanction (t-3)	54.76		0.20	57.39				
	(80.68)		(0.74)	(879.76)				
Sanction (t-4)	246.98**		0.00	362.01				
	(80.69)		(0.74)	(879.35)				
Sanction (t-5)			1.48*	335.37				
			(0.73)	(879.40)				
Sanction (t-6)			0.83	1196.34				
			(0.74)	(879.44)				
Sanction (t-7)			1.88*	1550.66				
			(0.74)	(879.98)				
Sanction (t-8)				1159.90				
				(880.98)				
Sanction (t-9)				1676.57				
				(890.18)				
Sanction (t-10)				2451.28**				
				(882.50)				
Sanction (t-11)				1657.51				
				(884.84)				
Sanction (t-12)				−799.73				
				(885.89)				
Sanction (t-13)				−461.04				
				(885.73)				
Sanction (t-14)				242.03				
				(885.35)				
Sanction threat	−33.82	−587.64	0.05	−262.30	43.64	−260.12	−6.59	63.56
	(84.96)	(563.49)	(0.55)	(770.15)	(49.33)	(945.83)	(69.71)	(1195.95)
Δ DoS (t-1)	−0.54***	−0.37***	−0.27***	−0.38***	−0.70***		−0.70***	
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)		(0.03)	
Δ DoS (t-2)	−0.49***	−0.36***	−0.20***	−0.37***	−0.64***		−0.64***	
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)		(0.03)	
Δ DoS (t-3)	−0.46***	−0.33***	−0.20***	−0.34***	−0.57***		−0.57***	
	(0.03)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-4)	−0.40***	−0.18***	−0.12***	−0.19***	−0.52***		−0.52***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-5)	−0.33***	−0.21***	−0.11***	−0.21***	−0.48***		−0.48***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-6)	−0.32***	−0.15***	−0.06*	−0.15***	−0.43***		−0.43***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-7)	−0.29***	−0.12***	−0.06*	−0.11***	−0.38***		−0.38***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-8)	−0.23***	−0.12***	−0.06*	−0.11***	−0.34***		−0.33***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-9)	−0.12**	−0.01	0.00	0.00	−0.29***		−0.29***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-10)	−0.13***	−0.08**	0.03	−0.06*	−0.26***		−0.26***	
	(0.04)	(0.03)	(0.03)	(0.03)	(0.04)		(0.04)	
Δ DoS (t-11)	−0.14***	−0.03	−0.01		−0.24***		−0.24***	
	(0.04)	(0.03)	(0.03)		(0.04)		(0.04)	
Δ DoS (t-12)	−0.11**	−0.04	−0.06*		−0.18***		−0.18***	
	(0.03)	(0.03)	(0.03)		(0.04)		(0.04)	
Δ DoS (t-13)	−0.06	−0.03	−0.00		−0.13***		−0.13***	
	(0.03)	(0.03)	(0.03)		(0.03)		(0.03)	
Δ DoS (t-14)	−0.01	−0.00	0.02		−0.08**		−0.08**	
	(0.03)	(0.03)	(0.03)		(0.03)		(0.03)	
R^2	0.27	0.18	0.11	0.19	0.34	0.44	0.34	0.44
Adj. R^2	0.26	0.17	0.09	0.17	0.33	0.44	0.33	0.44
Num. obs.	1388	1402	1368	1402	1375	1414	1375	1412
RMSE	299.60	2155.89	1.63	2148.69	167.52	2665.91	167.57	2669.17

Table E.4.5: Untransformed ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-02-13	Δ DoS US > 2012-02-13	Δ DoS US <= 2012-02-13 (techno.)	Δ DoS US > 2012-02-13 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction	0.12	0.40	0.36	0.06	0.44	0.64	0.71	1.31
	(0.43)	(0.46)	(0.81)	(0.68)	(0.32)	(0.54)	(0.51)	(0.72)
Sanction (t-1)	−0.20		−0.60	−0.40	0.22			0.56
	(0.44)		(0.81)	(0.68)	(0.31)			(0.72)
Sanction (t-2)	0.26		0.09	0.36	0.22			−1.24
	(0.45)		(0.81)	(0.68)	(0.31)			(0.72)
Sanction (t-3)	1.31**		1.80*	−0.08	0.55			−0.08
	(0.45)		(0.81)	(0.67)	(0.30)			(0.72)
Sanction (t-4)	1.17**		1.58*	0.80	−0.48			−1.34
	(0.43)		(0.70)	(0.67)	(0.30)			(0.72)
Sanction (t-5)				0.59	−0.53			1.95**
				(0.67)	(0.30)			(0.72)
Sanction (t-6)				0.06	−0.49			
				(0.68)	(0.30)			
Sanction (t-7)				1.63*				
				(0.74)				
Sanction (t-8)				1.48*				
				(0.74)				
Sanction (t-9)				1.01				
				(0.75)				
Sanction (t-10)				2.06**				
				(0.74)				
Sanction (t-11)				1.85*				
				(0.74)				
Sanction threat	−0.21	−0.38	0.11	−0.13	0.41	−0.88	−0.18	0.05
	(0.45)	(0.45)	(0.53)	(0.63)	(0.32)	(0.61)	(0.45)	(0.81)
Δ DoS (t-1)	−0.26***	−0.24***	−0.25***	−0.26***	−0.37***	−0.38***	−0.37***	−0.38***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.23***	−0.17***	−0.23***	−0.19***	−0.34***	−0.22***	−0.34***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-3)	−0.16***	−0.20***	−0.16***	−0.21***	−0.26***	−0.22***	−0.26***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-4)	−0.12***	−0.04	−0.12***	−0.06	−0.21***	−0.08*	−0.22***	−0.08*
	(0.03)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-5)	−0.08*	−0.09**	−0.08*	−0.10***	−0.18***	−0.10**	−0.19***	−0.10**
	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-6)	−0.11**	−0.06*	−0.11**	−0.07*	−0.16***	−0.13***	−0.18***	−0.13***
	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-7)	0.00	−0.06	0.01	−0.06*	−0.13***	−0.06	−0.13***	−0.07*
	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-8)	−0.04	−0.06	−0.04	−0.07*	−0.10**	−0.03	−0.10*	−0.03
	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-9)	−0.02	−0.02	−0.01	−0.02	−0.14***	−0.06	−0.13***	−0.07*
	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-10)	−0.00	−0.03	0.01	−0.03	−0.09*	−0.05	−0.09*	−0.05
	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-11)	−0.06	−0.00	−0.05	−0.00	−0.13***	−0.08*	−0.13***	−0.08**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-12)	−0.07	−0.03	−0.06	−0.02	−0.11**	−0.06	−0.11**	−0.06
	(0.03)	(0.03)	(0.03)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-13)	−0.03	−0.03	−0.03	−0.02	−0.02	0.01	−0.02	0.01
	(0.03)	(0.03)	(0.03)	(0.03)	(0.04)	(0.03)	(0.04)	(0.03)
Δ DoS (t-14)	0.05	0.06	0.05	0.05	−0.02	0.08**	−0.01	0.08**
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-15)		−0.03						
		(0.03)						
R^2	0.11	0.09	0.11	0.11	0.17	0.16	0.16	0.17
Adj. R^2	0.10	0.08	0.09	0.09	0.16	0.15	0.15	0.16
Num. obs.	976	1231	976	1239	970	1252	970	1252
RMSE	1.39	1.65	1.40	1.64	0.97	1.61	0.97	1.60

Table E.4.6: Without NAs ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-01-31	Δ DoS US > 2012-01-31	Δ DoS US <= 2012-01-31 (techno.)	Δ DoS US > 2012-01-31 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction	0.45	0.55	1.19	0.48	0.23	0.28	−0.47	1.43
	(0.54)	(0.46)	(0.91)	(0.68)	(0.46)	(0.63)	(0.67)	(0.83)
Sanction (t-1)	−0.03			1.56*	−0.67			
	(0.54)			(0.67)	(0.45)			
Sanction (t-2)	−1.18*			1.07				
	(0.53)			(0.68)				
Sanction threat	−0.19	−0.40	−0.58	0.30	0.36	−0.10	−0.05	0.42
	(0.56)	(0.43)	(0.68)	(0.59)	(0.44)	(0.67)	(0.61)	(0.83)
Δ DoS (t-1)	−0.39***	−0.11	−0.38***	−0.16*	−0.41***	−0.16*	−0.41***	−0.16*
	(0.07)	(0.07)	(0.07)	(0.07)	(0.07)	(0.07)	(0.07)	(0.07)
Δ DoS (t-2)	−0.21**		−0.22**		−0.19**	−0.07	−0.18*	−0.07
	(0.07)		(0.07)		(0.07)	(0.07)	(0.07)	(0.07)
R^2	0.16	0.05	0.15	0.06	0.16	0.03	0.15	0.04
Adj. R^2	0.14	0.03	0.13	0.03	0.14	0.01	0.13	0.02
Num. obs.	199	205	199	205	199	205	199	205
RMSE	1.92	1.62	1.92	1.61	1.44	1.84	1.45	1.82

Table E.4.7: Week ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

Δ DoS	Imposition	Threat	Model
21	4	0	US <= 2012-02-13
21	0	0	US > 2012-02-13
21	0	1	US (techno.) <= 2012-02-13
21	11	0	US (techno.) > 2012-02-13
21	6	0	EU <= 2012-01-31
21	0	2	EU > 2012-01-31
21	0	0	EU (techno.) <= 2012-01-31
21	5	0	EU (techno.) > 2012-01-31

Table E.4.8: Suggested lags when expanding maximal lag length to 21 days. Note: Models with best AIC values are chosen.

	Δ DoS US <= 2012-02-13	Δ DoS US > 2012-02-13	Δ DoS US <= 2012-02-13 (techno.)	Δ DoS US > 2012-02-13 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction	−0.48	0.48	−0.13	0.65	0.82	0.68	1.03	2.15*
	(0.52)	(0.59)	(0.85)	(0.82)	(0.48)	(0.67)	(0.58)	(0.95)
Sanction (t-1)		−0.46		−0.25				
		(0.59)		(0.82)				
Sanction (t-2)		−0.48		0.05				
		(0.59)		(0.81)				
Sanction (t-3)		0.38		−0.02				
		(0.59)		(0.81)				
Sanction (t-4)		0.06		0.68				
		(0.59)		(0.81)				
Sanction (t-5)				1.01				
				(0.81)				
Sanction (t-6)				0.58				
				(0.82)				
Sanction (t-7)				1.21				
				(0.82)				
Sanction (t-8)				1.12				
				(0.82)				
Sanction (t-9)				1.15				
				(0.84)				
Sanction (t-10)				1.97*				
				(0.82)				
Sanction (t-11)				1.80*				
				(0.82)				
Sanction (t-12)				−0.92				
				(0.82)				
Sanction (t-13)				−0.15				
				(0.82)				
Sanction (t-14)				0.44				
				(0.82)				
Sanction threat	−0.40	−1.00	−0.01	0.12	0.22	−1.54*	−0.08	−0.24
	(0.73)	(0.59)	(0.85)	(0.84)	(0.44)	(0.74)	(0.58)	(0.95)
Δ DoS (t-1)	−0.27***	−0.21***	−0.26***	−0.22***	−0.40***	−0.39***	−0.40***	−0.39***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.21***	−0.16***	−0.21***	−0.16***	−0.33***	−0.22***	−0.33***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.18***	−0.15***	−0.18***	−0.16***	−0.23***	−0.21***	−0.23***	−0.21***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.09**		−0.09**		−0.23***	−0.09**	−0.23***	−0.09**
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-5)	−0.05		−0.05		−0.16***	−0.08**	−0.16***	−0.08**
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-6)	−0.07*		−0.07*		−0.11***	−0.09**	−0.11***	−0.10**
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-7)	0.00		0.00		−0.09**	−0.03	−0.09**	−0.04
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-8)	−0.02		−0.02		−0.06	−0.00	−0.06	−0.00
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-9)	0.01		0.01		−0.07*	−0.03	−0.07*	−0.03
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-10)	0.02		0.03		−0.06*	−0.02	−0.06*	−0.01
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-11)	−0.05		−0.05		−0.10**	−0.04	−0.10**	−0.04
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-12)	−0.04		−0.04		−0.08**	−0.03	−0.08**	−0.03
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-13)	−0.02		−0.02		−0.03	0.02	−0.02	0.02
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-14)	0.06*		0.06*		−0.01	0.07**	−0.00	0.07**
	(0.03)		(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
R^2	0.10	0.08	0.10	0.08	0.17	0.16	0.17	0.15
Adj. R^2	0.09	0.07	0.09	0.07	0.16	0.15	0.16	0.14
Num. obs.	1388	1402	1388	1402	1375	1415	1375	1415
RMSE	1.46	1.62	1.46	1.63	1.16	1.64	1.16	1.64

Table E.4.9: Targeted Sanctions ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-02-13	Δ DoS US > 2012-02-13	Δ DoS US <= 2012-02-13 (techno.)	Δ DoS US > 2012-02-13 (techno.)	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31	Δ DoS EU <= 2012-01-31 (techno.)	Δ DoS EU > 2012-01-31 (techno.)
Sanction	0.41	0.17	−0.00	−0.02	0.41	0.45	0.69	1.39
	(0.46)	(0.55)	(0.73)	(0.94)	(0.42)	(0.68)	(0.68)	(0.95)
Sanction (t-1)	−0.20		−0.13	−0.81	0.58			1.02
	(0.46)		(0.73)	(0.94)	(0.41)			(0.95)
Sanction (t-2)	0.05		−0.38	0.86	0.05			−1.92*
	(0.46)		(0.73)	(0.94)	(0.41)			(0.95)
Sanction (t-3)	1.11*		1.08	−0.21	0.66			−0.86
	(0.46)		(0.73)	(0.94)	(0.41)			(0.95)
Sanction (t-4)	1.79***		2.50***	0.91	−0.48			−1.72
	(0.46)		(0.73)	(0.94)	(0.41)			(0.95)
Sanction (t-5)				0.25				2.43*
				(0.94)				(0.95)
Sanction (t-6)				−1.54				
				(0.94)				
Sanction (t-7)				0.89				
				(0.94)				
Sanction (t-8)				1.39				
				(0.94)				
Sanction (t-9)				0.16				
				(0.94)				
Sanction (t-10)				2.97**				
				(0.94)				
Sanction (t-11)				1.25				
				(0.94)				
Sanction (t-12)				0.23				
				(0.94)				
Sanction (t-13)				−1.01				
				(0.94)				
Sanction (t-14)				0.81				
				(0.94)				
Sanction threat	−0.27	0.52	−0.15	0.27	0.47	0.43	−0.16	0.40
	(0.55)	(0.61)	(0.73)	(0.81)	(0.39)	(0.74)	(0.58)	(0.82)
Sanction threat (t-1)			−1.55*					1.19
			(0.73)					(0.82)
Δ DoS (t-1)	−0.27***	−0.21***	−0.27***	−0.21***	−0.41***	−0.38***	−0.40***	−0.38***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.21***	−0.16***	−0.20***	−0.16***	−0.34***	−0.22***	−0.33***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.18***	−0.16***	−0.18***	−0.16***	−0.22***	−0.21***	−0.23***	−0.20***
	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.09***	−0.00	−0.09**		−0.22***	−0.09**	−0.23***	−0.08**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-5)	−0.05	−0.05	−0.04		−0.15***	−0.09**	−0.16***	−0.08**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-6)	−0.08**	−0.01	−0.07*		−0.10**	−0.10**	−0.11***	−0.09**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-7)	0.00	−0.00	0.01		−0.09**	−0.03	−0.09**	−0.03
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-8)	−0.02	−0.01	−0.02		−0.07*	−0.00	−0.06	−0.00
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-9)	0.00	0.06*	0.01		−0.08**	−0.03	−0.07*	−0.03
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-10)	0.02	0.01	0.03		−0.07*	−0.01	−0.07*	−0.02
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-11)	−0.06	0.05	−0.05		−0.10***	−0.04	−0.10**	−0.04
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-12)	−0.05	0.01	−0.05		−0.07*	−0.03	−0.08*	−0.02
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-13)	−0.03	−0.01	−0.02		−0.02	0.02	−0.02	0.03
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-14)	0.06*	0.07*	0.06*		−0.00	0.07**	−0.00	0.08**
	(0.03)	(0.03)	(0.03)		(0.03)	(0.03)	(0.03)	(0.03)
R^2	0.12	0.08	0.11	0.08	0.18	0.15	0.17	0.16
Adj. R^2	0.10	0.07	0.10	0.07	0.17	0.14	0.16	0.15
Num. obs.	1388	1402	1388	1402	1375	1415	1375	1415
RMSE	1.45	1.63	1.45	1.63	1.15	1.64	1.16	1.63

Table E.4.10: Low-intensity ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US <= 2012-02-13	Δ DoS US > 2012-02-13	Δ DoS EU <= 2012-01-31	Δ DoS EU > 2012-01-31
Sanction	−0.82	2.03	2.01	4.06*
	(1.45)	(1.62)	(1.16)	(1.65)
Sanction (t-1)	0.84	−0.07		0.05
	(1.45)	(1.62)		(1.65)
Sanction (t-2)	−0.69	0.21		−3.78*
	(1.45)	(1.62)		(1.65)
Sanction (t-3)	1.53	−0.45		−0.87
	(1.45)	(1.62)		(1.65)
Sanction (t-4)	3.14*	0.74		−3.71*
	(1.45)	(1.62)		(1.65)
Sanction (t-5)	3.16*	1.48		
	(1.45)	(1.62)		
Sanction (t-6)	4.10**	−2.08		
	(1.45)	(1.62)		
Sanction (t-7)	5.56***	−1.62		
	(1.46)	(1.62)		
Sanction (t-8)	−1.54	1.64		
	(1.46)	(1.62)		
Sanction (t-9)	−1.75	3.71*		
	(1.46)	(1.62)		
Sanction (t-10)	−3.31*	4.51**		
	(1.46)	(1.63)		
Sanction (t-11)	0.31	3.67*		
	(1.47)	(1.63)		
Sanction (t-12)	−3.00*	−0.82		
	(1.47)	(1.63)		
Sanction (t-13)	−2.46	−3.95*		
	(1.47)	(1.63)		
Sanction (t-14)		0.06		
		(1.63)		
Δ DoS (t-1)	−0.28***	−0.22***	−0.40***	−0.39***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-2)	−0.22***	−0.16***	−0.34***	−0.22***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-3)	−0.19***	−0.15***	−0.23***	−0.21***
	(0.03)	(0.03)	(0.03)	(0.03)
Δ DoS (t-4)	−0.10***		−0.23***	−0.08**
	(0.03)		(0.03)	(0.03)
Δ DoS (t-5)	−0.04		−0.16***	−0.07*
	(0.03)		(0.03)	(0.03)
Δ DoS (t-6)	−0.06*		−0.11***	−0.09**
	(0.03)		(0.03)	(0.03)
Δ DoS (t-7)	0.02		−0.09**	−0.03
	(0.03)		(0.03)	(0.03)
Δ DoS (t-8)	−0.01		−0.06	−0.00
	(0.03)		(0.03)	(0.03)
Δ DoS (t-9)	0.02		−0.07*	−0.03
	(0.03)		(0.03)	(0.03)
Δ DoS (t-10)	0.04		−0.07*	−0.02
	(0.03)		(0.03)	(0.03)
Δ DoS (t-11)	−0.04		−0.10***	−0.04
	(0.03)		(0.03)	(0.03)
Δ DoS (t-12)	−0.03		−0.08**	−0.03
	(0.03)		(0.03)	(0.03)
Δ DoS (t-13)	−0.01		−0.02	0.02
	(0.03)		(0.03)	(0.03)
Δ DoS (t-14)	0.05*		−0.00	0.07**
	(0.03)		(0.03)	(0.03)
Sanction threat			0.06	
			(1.17)	
R^2	0.13	0.09	0.17	0.16
Adj. R^2	0.12	0.07	0.16	0.15
Num. obs.	1388	1402	1375	1415
RMSE	1.44	1.62	1.16	1.64

Table E.4.11: High-intensity sanctions ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

	Δ DoS US > 2012-02-13 (techno.) - without Russia
Sanction	−0.31
	(0.73)
Sanction (t-1)	−0.65
	(0.73)
Sanction (t-2)	0.47
	(0.73)
Sanction (t-3)	0.03
	(0.73)
Sanction (t-4)	0.79
	(0.73)
Sanction (t-5)	0.37
	(0.73)
Sanction (t-6)	0.37
	(0.73)
Sanction (t-7)	2.14**
	(0.73)
Sanction (t-8)	1.06
	(0.73)
Sanction (t-9)	−0.39
	(0.74)
Sanction (t-10)	1.57*
	(0.73)
Sanction (t-11)	0.72
	(0.73)
Sanction (t-12)	−0.29
	(0.73)
Sanction (t-13)	0.84
	(0.73)
Sanction (t-14)	0.80
	(0.73)
Sanction threat	−0.18
	(0.58)
Δ DoS (t-1)	−0.21***
	(0.03)
Δ DoS (t-2)	−0.16***
	(0.03)
Δ DoS (t-3)	−0.16***
	(0.03)
R^2	0.08
Adj. R^2	0.07
Num. obs.	1402
RMSE	1.63

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$

Table E.4.12: Sanctions on techno. countries w/o Russia ARDL models. Note: $^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$.

Bibliography

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):235–247.

Athey, Susan and Markus Mobius. 2012. "The Impact of News Aggregators on Internet News Consumption: The Case of Localization." Working Paper. Harvard University and Iowa State University.

Baissa, Daniel K and Carlisle Rainey. 2018. "When BLUE is not Best: Non-normal Errors and the Linear Model." *Political Science Research and Methods* Online First:1–13.

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).

Beyer, Jessica L. 2014. *Expect us: Online Communities and Political Mobilization.* Oxford: Oxford University Press.

Blei, David M, Andrew Y Ng and Michael I Jordan. 2003. "Latent Dirichlet Allocation." *Journal of Machine Learning Research* 3(Jan):993–1022.

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*, ed. John Zysman and Abraham Newman. Stanford, CA: Stanford University Press.

Breuer, Anita, Todd Landman and Dorothea Farquhar. 2015. "Social Media and Protest Mobilization: Evidence from the Tunisian Revolution." *Democratization* 22(4):764–792.

Brutlag, Jake. 2009. "Speed Matters for Google Web Search." *Google.* `https://services.google.com/fh/files/blogs/google_delayexp.pdf` (accessed 07-29-2019).

Burnham, Kenneth P and David R Anderson. 2004. "Multimodel Inference: Understanding AIC and BIC in Model Selection." *Sociological Methods & Research* 33(2):261–304.

Butler, Daren. 2011. "Turkish Websites Attacked by Anonymous Before Vote." *Reuters*, June 09. https://www.reuters.com/article/us-turkey-election-internet/turkish-websites-attacked-by-anonymous-before-vote-idUSTRE7583DV20110609 (accessed 29-07-2019).

CAIDA, UC San Diego. 2016. "The CAIDA UCSD Near-Real-Time Network Telescope - 2008-2016.". 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." *Journalism in the Americas*. https://knightcenter.utexas.edu/blog/00-18194-freedom-press-also-targeted-virtually-venezuela-where-cyberattacks-can-force-independe (accessed 29-07-2019).

Carr, Jeffrey. 2011. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media.

Caruso, Raul. 2003. "The Impact of International Economic Sanctions on Trade: An Empirical Analysis." *Peace Economics, Peace Science and Public Policy* 9(2):1–34.

Casey, Nicholas. 2018. "Venezuela's Most-wanted Rebel Shared His Story, just before Being Gunned Down." *The Independent*, February 02. https://www.independent.co.uk/news/long_reads/oscar-perez-death-venezuela-helicopter-attack-caracas-muerte-suspendida-a8177051.html (accessed 07-29-2019).

Chen, Yuyu and David Y Yang. 2019. "The Impact of Media Censorship: 1984 or Brave New World?" *American Economic Review* 109(6):2294–2332.

Cherney, Max. 2014. "Pro-Russian Hackers Took Down Three NATO Websites. The work of Russian cyber-agent provocateurs?" *Motherboard*, March 16. https://motherboard.vice.com/en_us/article/jp5mxd/pro-russia-ukranians-hack-nato-websites (accessed 07-29-2019).

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York, NY: Verso Books.

Cook, Scott J, Jude C Hays and Robert J Franzese. 2018. "Fixed Effects in Rare Events Data: A Penalized Maximum Likelihood Solution." *Political Science Research and Methods* Online First:1–14.

Coppedge, Michael, John Gerring, Staffan I. Lindberg, Svend-Erik Skaaning, Jan Teorell, David Altman, Michael Bernhard, M. Steven Fish, Adam Glynn, Allen Hicken, Carl Henrik Knutsen, Kyle Marquardt, Kelly McMann, Farhad Miri, Pamela Paxton, Daniel Pemstein, Jeffrey Staton, Eitan Tzelgov, Yi-ting Wang and Brigitte Zimmerman. 2016. "V-Dem [Country-Year/Country-Date] Datatset v6.2.". University of Gothenburg: Varieties of Democracy (V-Dem) Project.

Cortright, David, George A Lopez, Richard W Conroy, Jaleh Dashti-Gibson, Julia Wagler, David M Malone and Lloyd Axworthy. 2000. *The Sanctions Decade: Assessing UN Strategies in the 1990s*. Vol. 1 Boulder, CO: Lynne Rienner Publishers.

Crabtree, Charles, Christopher J Fariss and Holger L Kern. 2015. "Truth Replaced by Silence: A Field Experiment on Private Censorship in Russia." Working Paper. Available at SSRN: `https://ssrn.com/abstract=2708274` or `http://dx.doi.org/10.2139/ssrn.2708274`.

Cranmer, Skyler J, Tobias Heinrich and Bruce A Desmarais. 2014. "Reciprocity and the Structural Determinants of the International Sanctions Network." *Social Networks* 36:5–22.

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):1964–1977.

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.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain and Janice Gross Stein. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Boston: MIT Press.

Deibert, Ronald and Rafal Rohozinski. 2010. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21(4):43–57.

Diamond, Larry. 2010. "Liberation Technology." *Journal of Democracy* 21(3):69–83.

Dolata, Ulrich and Jan-Felix Schrape. 2016. "asses, 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.

Edmond, Chris. 2013. "Information Manipulation, Coordination, and Regime Change." *Review of Economic Studies* 80(4):1422–1458.

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` or `http://dx.doi.org/10.2139/ssrn.2696236`.

Escribà-Folch, Abel and Joseph Wright. 2010. "Dealing with Tyranny: International Sanctions and the Survival of Authoritarian Rulers." *International Studies Quarterly* 54(2):335–359.

Firth, David. 1993. "Bias Reduction of Maximum Likelihood Estimates." *Biometrika* 80(1):27–38.

Fisher, Max and Jared Keller. 2011. "Syria's Digital Counter-Revolutionaries." *The Atlantic*. `https://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/` (accessed 29-07-2019).

Frantz, Erica and Andrea Kendall-Taylor. 2014. "A Dictator's Toolkit Understanding how Co-optation Affects Repression in Autocracies." *Journal of Peace Research* 51(3):332–346.

Freedom House. 2016. "Freedom of the Net 2016: Silencing the Messenger: Communication Apps Under Pressure." Washington, DC.

Freedom House. 2017*a*. "Freedom of the Press 2017: Press Freedom's Dark Horizon." Washington, DC.

Freedom House. 2017*b*. "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy." Washington, DC.

Freedom House. 2018. "Freedom on the Net 2018: The Rise of Digital Authoritarianism." Washington, DC.

Friedrich, Carl J and Zbigniew K Brzezinski. 1965. *Totalitarian Dictatorship*. Cambridge, MA: Harvard University Press.

Galtung, Johan. 1967. "On the Effects of International Economic Sanctions, with Examples from the Case of Rhodesia." *World Politics* 19(3):378–416.

Gandhi, Jennifer and Ellen Lust-Okar. 2009. "Elections under Authoritarianism." *Annual Review of Political Science* 12:403–422.

Gardner, G, Andrew C Harvey and Garry DA Phillips. 1980. "Algorithm AS 154: An Algorithm for Exact Maximum Likelihood Estimation of Autoregressive-moving Average Models by Means of Kalman Filtering." *Journal of the Royal Statistical Society. Series C (Applied Statistics)* 29(3):311–322.

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

Geddes, Barbara and John Zaller. 1989. "Sources of Popular Support for Authoritarian Regimes." *American Journal of Political Science* 33(2):319–347.

Geddes, Barbara, Joseph Wright and Erica Frantz. 2014. "Autocratic Breakdown and Regime Transitions: A New Data Set." *Perspectives on Politics* 12(2):313–331.

Geers, Kenneth, Darien Kindlund, Ned Moran and Rob Rachwald. 2014. "WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks." *FireEye*. `https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf` (accessed 06-28-2019).

Gilbert, David. 2019. "Inside the massive cyber war between Russia and Ukraine." *Vice*, March 29. `https://news.vice.com/en_us/article/bjqe8m/inside-the-massive-cyber-war-between-russia-and-ukraine` (accessed 07-29-2019).

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

Gohdes, Anita R. 2015. "Pulling the Plug: Network Disruptions and Violence in Civil Conflict." *Journal of Peace Research* 52(3):352–367.

Goncharov, Max. 2012. "Russian Underground 101." *Trend Micro Incorporated*. `https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf` (accessed 29-07-2019).

Grauvogel, Julia, Amanda A Licht and Christian von Soest. 2017. "Sanctions and Signals: How International Sanction Threats Trigger Domestic Protest in Targeted Regimes." *International Studies Quarterly* 61(1):86–97.

Grauvogel, Julia and Christian Von Soest. 2014. "Claims to Legitimacy Count: Why Sanctions Fail to Instigate Democratisation in Authoritarian Regimes." *European Journal of Political Research* 53(4):635–653.

Greene, William H. 2011. *Econometric Analysis*. Vol. 7 London: Pearson.

Grimmer, Justin and Brandon M Stewart. 2013. "Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts." *Political Analysis* 21(3):267–297.

Gross, Michael L, Daphna Canetti and Dana R Vashdi. 2017. "Cyberterrorism: Its Effects on Psychological Well-being, Public Confidence and Political Attitudes." *Journal of Cybersecurity* 3(1):49–58.

Gueorguiev, Dimitar D. and Edmund J. Malesky. 2019. "Consultation and Selective Censorship in China." *The Journal of Politics* Online First:1–7.

Gunitsky, Seva. 2015. "Corrupting the Cyber-commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13(01):42–54.

Haass, Richard N. 1997. "Sanctioning Madness." *Foreign Affairs* 76(6):74–85.

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 *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association pp. 527–541.

Hassanpour, Navid. 2014. "Media Disruption and Revolutionary Unrest: Evidence From Mubarak's Quasi-Experiment." *Political Communication* 31(1):1–24.

Hathaway, Oona A, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel. 2012. "The Law of Cyber-attack." *California Law Review* pp. 817–885.

Hawkins, DM and S Weisberg. 2017. "Combining the Box-cox Power and Generalised Log Transformations to Accommodate Nonpositive Responses in Linear and Mixed-effects Linear Models." *South African Statistical Journal* 51(2):317–328.

Hawkins, Kirk A. 2016. "Chavismo, Liberal Democracy, and Radical Democracy." *Annual Review of Political Science* 19(1):311–329.

Hedberg, Masha. 2018. "The Target Strikes Back: Explaining Countersanctions and Russia's Strategy of Differentiated Retaliation." *Post-Soviet Affairs* 34(1):35–54.

Hellmeier, Sebastian. 2016. "The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes." *Politics & Policy* 44(6):1158–1191.

Hellmeier, Sebastian. 2019. "From External Pressure to Internal Cohesion - Rally Effects in Authoritarian Regimes." Unpublished Working Paper. University of Konstanz.

Hendry, David F. 1995. *Dynamic Econometrics*. Oxford: Oxford University Press.

Hobbs, William R and Margaret E Roberts. 2018. "How Sudden Censorship Can Increase Access to Information." *American Political Science Review* 112(3):621–636.

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):356–373.

Howard, Philip N and Muzammil M Hussain. 2011. "The Role of Digital Media." *Journal of Democracy* 22(3):35–48.

Howard, Philip N, Sheetal D Agarwal and Muzammil M Hussain. 2011. "When do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media." *The Communication Review* 14(3):216–232.

IFES ElectionGuide. 2017. "ElectionGuide: Democracy Assistance & Election News.". `https://www.electionguide.org` (accessed 07-29-2019).

Internet Society. 2015. "Adressing the Challenge of IP Spoofing.". `https://www.internetsociety.org/doc/addressing-challenge-ip-spoofing` (accessed 07-29-2019).

ITU, International Communication Union. 2017. "The ICT Development Index (IDI): Conceptual Framework and Methodology.". `https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx`.

Jagannathan, Malavika. 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, 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*. IMC '17 New York, NY, USA: ACM pp. 100–113.

Jordan, Tim. 2002. *Activism!: Direct Action, Hacktivism and the Future of Society*. London: Reaktion books.

Kaempfer, William H, Anton D Lowenberg and William Mertens. 2004. "International Economic Sanctions Against a Dictator." *Economics & Politics* 16(1):29–51.

Karnej, Ihar and Brian Whitmore. 2008. "Belarus: RFE/RL Cites Online 'Solidarity' In Face Of Cyberattack." *Radio Free Europe*, April 29. `https://www.rferl.org/a/1109649.html` (accessed 07-29-2019).

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.

King, Gary, Robert O Keohane and Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press.

Klyueva, Anna. 2016. "Taming online political engagement in Russia: Disempowered publics, empowered state and challenges of the fully functioning society." *International Journal of Communication* 10:20.

Knutsen, Carl Henrik, Håvard Mokleiv 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):317–347.

Kuran, Timur. 1991. "Now Out of Never: The Element of Surprise in the East European Revolution of 1989." *World Politics* 44(1):7–48.

Levitsky, Steven and James Loxton. 2013. "Populism and Competitive Authoritarianism in the Andes." *Democratization* 20(1):107–136.

Levitsky, Steven and Lucan A Way. 2010. *Competitive authoritarianism: Hybrid regimes after the Cold War*. Cambridge University Press.

Lindberg, Steffan I. 2009. *Democratization by Election: A New Mode of Transition*. Baltimore, MD: Johns Hopkins University Press.

Ling, Justin. 2016. "Black Lives Matter Website Saw Over 100 DDoS Attacks in Seven Months." *Vice*. `https://www.vice.com/en_us/article/wnxbv5/black-lives-matter-website-ddos-ghost-squad-hacking` (accessed 07-29-2019).

Little, Andrew T. 2012. "Elections, Fraud, and Election Monitoring in the Shadow of Revolution." *Quarterly Journal of Political Science* 7(3):249–283.

Little, Andrew T. 2016. "Communication Technology and Protest." *The Journal of Politics* 78(1):152–166.

Lone, Q., M. Luckie, M. Korczyński and M. van Eeten. 2017. Using Loops Observed in Traceroute to Infer the Ability to Spoof. In *Passive and Active Measurement Conference (PAM)*.

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):X–X.

Lupia, Arthur and Gisela Sin. 2003. "Which Public Goods Are Endangered?: How Evolving Communication Technologies Affect the Logic of Collective Action." *Public Choice* 117:315–331.

Lutscher, Philipp M, Nils B Weidmann, Margaret E Roberts, Mattijs Jonker, Alistair King and Alberto Dainotti. 2020. "At Home and Abroad: The Use of Denial-of-Service Attacks During Elections in Nondemocratic Regimes." *Journal of Conflict Resolution* 64(2-3):373–401.

Lynn III, William F. 2010. "Defending a New Domain-the Pentagon's Cyberstrategy." *Foreign Affairs* 89(5):97–108.

MacKinnon, Rebecca. 2013. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, NY: Basic Books.

Magaloni, Beatriz. 2008. "Credible Power-sharing and the Longevity of Authoritarian Rule." *Comparative Political Studies* 41(4-5):715–741.

Maggi, Federico, Marco Balduzzi, Ryan Flores, Lion Gu and Vincenzo Ciancaglini. 2018. Investigating Web Defacement Campaigns at Large. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ASIACCS '18 New York, NY: ACM pp. 443–456.

Maness, Ryan C and Brandon Valeriano. 2016. "The Impact of Cyber Conflict on International Interactions." *Armed Forces & Society* 42(2):301–323.

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert and Vern Paxson. 2015. An Analysis of China's "Great Cannon". In *5th USENIX Workshop on Free and Open Communications on the Internet (FOCI 15)*. Washington, D.C.: USENIX Association.

Marinov, Nikolay. 2005. "Do Economic Sanctions Destabilize Country Leaders?" *American Journal of Political Science* 49(3):564–576.

Marshall, Monty G and Keith Jaggers. 2016. "Polity IV Project: Political Regime Characteristics and Transitions, 1800-2016.". Vienna, VA: Center for Systemic Peace.

Martin, Brian. 2005. "Researching Nonviolent Action: Past Themes and Future Possibilities." *Peace & Change* 30(2):247–270.

Martin, Brian. 2007. *Justice Ignited: The Dynamics of Backfire*. Lanham, MD: Rowman & Littlefield.

Matthews, Tim. 2014. "Incapsula Survey : What DDoS Attacks Really Cost Businesses." *Incapsula*. https://lp.incapsula.com/rs/incapsulainc/images/eBook20-20DDoS20Impac20Survey.pdf (accessed 29-07-2019).

McAdam, Doug. 1983. "Tactical Innovation and the Pace of Insurgency." *American Sociological Review* 48(6):735–754.

McLellan, Charles. 2018. "Cyberwar Predictions for 2019: The Stakes Have Been Raised." *ZDNet*. https://www.zdnet.com/article/cyberwar-predictions-for-2019-the-stakes-have-been-raised/ (accessed 07-30-2019).

Milan, Stefania. 2015. Hacktivism as a Radical Media Practice. In *Routledge Companion to Alternative and Community Media*, ed. Chris Atton. London: Routledge pp. 550–560.

Mitchelstein, Eugenia and Pablo J Boczkowski. 2009. "Between Tradition and Change: A Review of Recent Research on Online News Production." *Journalism* 10(5):562–586.

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):115–139.

Moritz, Steffen and Thomas Bartz-Beielstein. 2017. "*imputeTS*: Time Series Missing Value Imputation in R." *The R Journal* 9(1):207–218.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. 1st ed. New York, NY: PublicAffairs.

Munger, Kevin, Richard Bonneau, Jonathan Nagler and Joshua A Tucker. 2018. "Elites Tweet to Get Feet Off the Streets: Measuring Regime Social Media Strategies During Protest." *Political Science Research and Methods* pp. 1–20. Online First.

Nazario, Jose. 2009. Politically Motivated Denial of Service Attacks. In *The Virtual Battlefield: Perspectives on Cyber Warfare*, ed. Christian Czosseck and Kenneth Geers. Amsterdam/Washington, DC: IOS Press pp. 163–181.

Netscout. 2017. "Insight into the Global Threat Landscape." *Netcout Arbor*. https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf (accessed 10-03-2019).

Nye Jr, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3):44–71.

Olson, Parmy. 2013. *We are Anonymous*. New York, NY: Back Bay Books/Little, Brown and Company.

Olson, Parmy. 2014. "The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites." *Forbes Magazine*, November 20. https://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/ (accessed 30-07-2019).

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).

Pagliery, Jose. 2018. "US banks Prepare for Iranian Cyberattacks as Retaliation for Sanctions.". https://edition.cnn.com/2018/11/09/tech/iran-sanctions-us-banks-cyber-hack-invs/index.html (accessed 07-30-2019).

Pape, Robert A. 1997. "Why Economic Sanctions Do Not Work." *International Security* 22(2):90–136.

Partyvan. 2012. "Operation Reasonable Reaction.". https://web.archive.org/web/20120425233420/http://partyvan.info/wiki/Operation_Reasonable_Reaction (accessed 07-30-2019).

PAT Research. 2019. "Top 16 Content Delivery Network Providers.". https://www.predictiveanalyticstoday.com/top-content-delivery-network-providers/ (accessed 07-30-2019).

Pearce, Katy E. and Sarah Kendzior. 2012. "Networked Authoritarianism and Social Media in Azerbaijan." *Journal of Communication* 62(2):283–298.

Pearce, Paul, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver and Vern Paxson. 2017. Global Measurement of DNS Manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association pp. 307–323.

Peksen, Dursun. 2009. "Better or Worse? The Effect of Economic Sanctions on Human Rights." *Journal of Peace Research* 46(1):59–77.

Perlroth, Nicole and Quentin Hardy. 2013. "Bank Hacking Was the Work of Iranians, Officials Say.". https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (accessed 07-30-2019).

Pesaran, M Hashem, Yongcheol Shin and Richard J Smith. 2001. "Bounds Testing Approaches to the Analysis of Level Relationships." *Journal of Applied Econometrics* 16(3):289–326.

Pettitt, AN. 1979. "A Non-parametric Approach to the Change-point Problem." *Journal of the Royal Statistical Society: Series C (Applied Statistics)* 28(2):126–135.

Philips, Andrew Q. 2018. "Have Your Cake and Eat It Too? Cointegration and Dynamic Inference from Autoregressive Distributed Lag Models." *American Journal of Political Science* 62(1):230–244.

Poznansky, Michael and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3(4):402–416.

Quinn, Kevin M, Burt L Monroe, Michael Colaresi, Michael H Crespin and Dragomir R Radev. 2010. "How to Analyze Political Attention with Minimal Assumptions and Costs." *American Journal of Political Science* 54(1):209–228.

Qurium, The Media Foundation. 2017. "News media Websites Attacked from Governmental Infrastructure in Azerbaijan.". `https://www.qurium.org/news-media-websites-attacked-from-governmental-infrastructure-in-azerbaijan/` (accessed 07-30-2019).

Radware. 2019. "How Cyberattacks Directly Impact Your Brand.". `https://blog.radware.com/security/applicationsecurity/2019/01/how-cyberattacks-directly-impact-your-brand-new-radware-report/` (accessed 07-30-2019).

Richard, Clarke, Knake Robert et al. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York, NY: HarperCollins Publishers.

Richter, Philipp, Ramakrishna Padmanabhan, Neil Spring, Arthur Berger and David Clark. 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.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35(1):5–32.

Rid, Thomas and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38(1-2):4–37.

Roberts, Hal and Bruce Etling. 2011. "Coordinated DDoS Attack During Russian Duma Elections." *Internet & Democracy Blog*, December 08. `http://blogs.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/` (accessed 30-07-2019).

Roberts, Margaret E. 2018. *Censored: Distraction and Diversion Inside Chinas Great Firewall*. Princeton, NJ: Princeton University Press.

Rød, Espen Geelmuyden and Nils B Weidmann. 2015. "Empowering Activists or Autocrats? The Internet in Authoritarian Regimes." *Journal of Peace Research* 52(3):338–351.

Rosas, Ronny. 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, Arturas and Denis Stukal. 2019. "How Autocrats Manipulate Economic News: Evidence from Russia's State-Controlled Television." *Journal of Politics* . Online First.

Sanovich, Sergey, Denis Stukal and Joshua A Tucker. 2018. "Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia." *Comparative Politics* 50(3):435–482.

Sauter, Molly. 2014. *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. Bloomsbury Publishing USA.

Schedler, Andreas. 2013. *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford: Oxford University Press.

Schmidt, Eric and Jared Cohen. 2016. "We Must Prepare Ourselves for the Cyberwars of the Future." *Time Ideas*. `http://time.com/4606057/cyberwars-of-the-future/`(accessed 07-30-2019).

Scott, James C. 1985. *Weapons of the Weak: Everyday Forms of Resistance*. New Haven, CT: Yale 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 (USENIX ATC 16)*. Denver, CO: USENIX Association pp. 195–208.

Sen, Ashish Kumar. 2018. "Venezuela's Sham Election." *Atlantic Council*. `http://www.atlanticcouncil.org/blogs/new-atlanticist/venezuela-s-sham-election` (accessed 30-7-2019).

Shadmehr, Mehdi and Dan Bernhardt. 2015. "State Censorship." *American Economic Journal: Microeconomics* 7(2):280–307.

Shakarian, Paulo, Jana Shakarian and Andrew Ruef. 2013. *Introduction to cyber-warfare: A multidisciplinary approach*. Oxford: Newnes.

Shanapinda, Stanley. 2019. "How a Cyber Attack Hampered Hong Kong Protesters." *The Conversation*, June 14. `https://theconversation.com/how-a-cyber-attack-hampered-hong-kong-protesters-118770` (accessed 08-14-2019).

Shi, Tian, Kyeongpil Kang, Jaegul Choo and Chandan K. Reddy. 2018. Short-Text Topic Modeling via Non-negative Matrix Factorization Enriched with Local Word-Context Correlations. In *Proceedings of the 2018 World Wide Web Conference*. WWW '18 Geneva: International World Wide Web Conferences Steering Committee pp. 1105–1114.

Shirah, Ryan. 2016. "Electoral Authoritarianism and Political Unrest." *International Political Science Review* 37(4):470–484.

Singer, J David. 1988. "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816–1985." *International Interactions* 14(2):115–132.

Spaiser, Viktoria, Thomas Chadefaux, Karsten Donnay, Fabian Russmann and Dirk Helbing. 2017. "Communication Power Struggles on Social Media: A Case Study of the 2011–12 Russian Protests." *Journal of Information Technology & Politics* 14(2):132–153.

Sundberg, Ralph and Erik Melander. 2013. "Introducing the UCDP Georeferenced Event Dataset." *Journal of Peace Research* 50(4):523–532.

Svolik, Milan. 2012. *The Politics of Authoritarian Rule*. Cambridge: Cambridge University Press.

Tarrow, Sidney and Charles Tilly. 2007. *Contentious Politics and Social Movements*. Oxford: Oxford University Press.

The Australian. 2011. "Malaysian News Site Attacked." *The Australian*, April 14. `https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:52M4-C3J1-F0JP-W0HJ-00000-00&context=1516831` (accessed 08-06-2019).

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).

Tilly, Charles. 1986. *The Contentious French: Four Centuries of Popular Struggle*. Cambridge, MA: Harvard University Press.

Tilly, Charles. 2003. *The Politics of Collective Violence*. Cambridge: Cambridge University Press.

Tilly, Charles, Douglas McAdam and Sidney Tarrow. 2001. *Dynamics of Contention*. Cambridge: Cambridge University Press.

Tucker, Joshua A. 2007. "Enough! Electoral Fraud, Collective Action Problems, and Post-communist Colored Revolutions." *Perspectives on Politics* 5(03):535–551.

Tucker, Joshua A, Yannis Theocharis, Margaret E Roberts and Pablo Barberá. 2017. "From Liberation to Turmoil: Social Media and Democracy." *Journal of Democracy* 28(4):46–59.

Tufekci, Zeynep. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven, CT: Yale University Press.

Tufekci, Zeynep and Christopher Wilson. 2012. "Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square." *Journal of Communication* 62:363–379.

Valeriano, Brandon, Benjamin M Jensen and Ryan C Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Valeriano, Brandon and Ryan C Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11." *Journal of Peace Research* 51(3):347–360.

Van Laer, Jeroen and Peter Van Aelst. 2010. "Internet and Social Movement Action Repertoires: Opportunities and Limitations." *Information, Communication & Society* 13(8):1146–1171.

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):1877–1888.

VanderSloot, Benjamin, Allison McDonald, Will Scott, J. Alex Halderman and Roya Ensafi. 2018. Quack: Scalable Remote Measurement of Application-Layer Censorship. In *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association pp. 187–202.

Veebel, Viljar and Raul Markus. 2018. "The Bust, the Boom and the Sanctions in Trade Relations with Russia." *Journal of International Studies* 11(1):9–20.

Verstraeten, Gert, Jean Poesen, Gaston Demarée and Christian Salles. 2006. "Long-term (105 years) Variability in Rain Erosivity as Derived From 10-min Rainfall Depth Data for Ukkel (Brussels, Belgium): Implications for Assessing Soil Erosion Rates." *Journal of Geophysical Research: Atmospheres* 111(D22).

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*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain. Boston: MIT Press pp. 153–176.

Vittinghoff, Eric and Charles E McCulloch. 2007. "Relaxing the Rule of Ten Events per Variable in Logistic and Cox Regression." *American Journal of Epidemiology* 165(6):710–718.

Volz, Dustin. 2018. "U.S. Charges, Sanctions Iranians for Global Cyber Attacks on Behalf of Tehran." *Reuters*, March 23. `https://www.reuters.com/article/us-usa-cyber-iran/u-s-charges-sanctions-iranians-for-global-cyber-attacks-on-behalf-of-tehran-idUSKBN1GZ22K` (accessed 07-30-2019).

Walker, Henry A, Larry Rogers and Morris Zelditch Jr. 1988. "Legitimacy and Collective Action: A Research Note." *Social Forces* 67(1):216–228.

Webb, Clayton. 2018. "Power Politics or Public Pandering? An Empirical Investigation of Economic Sanctions and Presidential Approval." *International Interactions* 44(3):491–509.

Weber, Patrick M. and Gerald Schneider. 2019. "Making the World Safe for Liberalism? Evaluating the Western Sanctions Regime with a New Dataset." Unpublished Working Paper. University of Konstanz.

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.

Weinberg, Zachary, Mahmood Sharif, Janos Szurdi and Nicolas Christin. 2017. "Topics of Controversy: An Empirical Analysis of Web Censorship Lists." *Proceedings on Privacy Enhancing Technologies* 2017(1):42–61.

Whang, Taehee. 2011. "Playing to the Home Crowd? Symbolic Use of Economic Sanctions in the United States." *International Studies Quarterly* 55(3):787–801.

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.

Wintrobe, Ronald. 2000. *The Political Economy of Dictatorship*. Cambridge: Cambridge University Press.

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):1015–1033.

Wood, Reed M. 2008. "A Hand Upon the Throat of the Nation: Economic Sanctions and State Repression, 1976–2001." *International Studies Quarterly* 52(3):489–513.

Wooldridge, Jeffrey M. 2015. *Introductory Econometrics: A Modern Approach*. Toronto: Nelson Education.

Woolf, Nicky. 2016. "DDoS Attack that Disrupted Internet Was Largest of Its Kind in History, Experts Say." *The Guardian*. `https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet` (accessed 30-07-2019).

World Bank. 2019. *World Development Indicators*. World Bank.

Xu, Yiqing. 2017. "Generalized Synthetic Control Method: Causal Inference with Interactive Fixed Effects Models." *Political Analysis* 25(1):57–76.

Xun, G., V. Gopalakrishnan, F. Ma, Y. Li, J. Gao and A. Zhang. 2016. Topic Discovery for Short Texts Using Word Embeddings. In *2016 IEEE 16th International Conference on Data Mining (ICDM)*. pp. 1299–1304.

Yan, Xiaohui, Jiafeng Guo, Yanyan Lan and Xueqi Cheng. 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.

Yildirim, A Kadir. 2016. *Muslim Democratic Parties in the Middle East: Economy and Politics of Islamist Moderation*. Bloomington, ID: 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):2046–2069.

Zeitzoff, Thomas. 2017. "How Social Media is Changing Conflict." *Journal of Conflict Resolution* 61(9):1970–1991.

Zuckerman, Ethan, Hal Roberts, Ryan McGrady, Jillian York and John Palfrey. 2010. "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites." Boston, MA: The Berkman Center for Internet & Society, Harvard University.