Journal of Global Security Studies, 6(4), 2021, 1–11
https://doi.org/10.1093/jogss/ogab001
Research Innovation

Digital Retaliation? Denial-of-Service Attacks after Sanction Events

Philipp M. Lutscher [1,2]

[1]University of Oslo, Department of Political Science, and [2]University of Konstanz, Department of Politics and Public Administration

Abstract

Conventional wisdom expects to see a rise in cyber activities around aggressive foreign policy events. In this article, I test this claim by investigating whether sanctions lead to an increase in denial-of-service (DoS) attacks using new data on DoS attacks measured from Internet traffic. Exploring the development of DoS attacks around sanctions imposed against Russia in 2014 indeed shows an increase of DoS attacks against several sanction sender states. Extending this case study to a systematic analysis, including all sanction threats and impositions made by the United States and the European Union between 2008 and 2016, shows no apparent patterns. When I exclusively consider sanctions against technologically advanced countries, however, the frequency of attacks rises systematically against the United States. It thus appears that states do not always have to expect a digital retaliation after aggressive foreign policies. Nevertheless, sanctioning countries may have to anticipate an increase in DoS attacks when their governments impose sanctions against technologically advanced countries.

Keywords: cyberattacks, sanctions, internet measurement

Introduction

On November 5, 2018, CNN reported that US banks prepared themselves for anticipated cyberattacks when the US government reinstated sanctions against Iran (Pagliery 2018).[1] Many news outlets, security pundits, and the public indeed expect a rise in cyberattacks after aggressive foreign policy events such as sanctions. This appears to be especially true for low-cost cyber actions, of which so-called denial-of-service (DoS) attacks are the most frequent type. This brute-force and technically simple cyber action overloads a server by flooding it with high levels of data traffic and rendering it temporally not reachable. Despite the simplicity of these attacks, they are a threat to international security as they can cause high economic costs, especially when they target industry and financial services (Matthews 2014).

There are several examples of DoS attacks related to international disputes. DoS attacks rose against news, government, and industry websites during the 2008 Russo-Georgian War (Deibert, Rohozinski, and Crete-Nishihata 2012), or were supposedly launched to retaliate sanctions against Iran (Perlroth and Hardy 2013). Previous empirical work illustrates that DoS attacks are one of the most commonly used types of cyberattacks between adversary states (Valeriano and Maness 2014). Nevertheless, there has yet not been a

1 In this paper, I use the terms cyberattack, cyber action, and cyber operation interchangeably. In defining these terms, I follow Hathaway et al. (2012) who state that "[a] cyber attack consists of any action taken to undermine the function of a computer network for a political or national security purposes."

Lutscher, Philipp M. (2020) Digital Retaliation? Denial-of-Service Attacks after Sanction Events. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogab001

systematic investigation of whether aggressive foreign policy events increase the frequency of DoS attacks.

In this paper, I investigate whether DoS attacks against sanction sending countries rise when they threaten or impose sanctions. My investigation advances previous research in two ways. First, I systematically explore international political drivers of DoS attacks focusing on sanctions as one of the likeliest cases for which one should expect such attacks.[2] Second, instead of collecting data on DoS attacks from media sources, I rely on a dataset of DoS attacks measured from Internet traffic to gain a more comprehensive picture of the development and intensity of DoS attacks on countries worldwide (CAIDA 2016).

I start exploring this relationship by focusing on sanctions against Russia in 2014 as a most likely case to expect a digital retaliation. This investigation shows compelling evidence for an increase in DoS attacks against the main sanctioning entities, the United States and the European Union (EU), as well as other sanctioning countries. To explore how systematic this relationship is, I run time series models considering all sanction threats and impositions made by the United States and the EU from 2008 until the beginning of 2016 on a daily level. The results show no apparent patterns. However, when I restrict the analysis to sanctions against technologically advanced countries—which can be assumed to have higher cyber capabilities—I find a significant positive correlation between sanction impositions and DoS attacks against the United States. This research innovation thus illustrates that not every aggressive foreign policy leads to a digital retaliation. The study's results nevertheless suggest that the number of DoS attacks may increase against sanction sending countries when they target technologically advanced states—additional costs governments need to consider when imposing sanctions against foreign countries.

This article proceeds as follows. First, building on the literature on emotions in international relations (Sasley 2011) and previous works on politically motivated DoS attacks (e.g., Deibert, Rohozinski, and Crete-Nishihata 2012; Asal et al. 2016; Valeriano, Jensen, and Maness 2018; Kostyuk and Zhukov 2019), I discuss why the frequency of DoS attacks should increase against countries when they threaten or impose sanctions. Afterward, I introduce the data on DoS attacks and sanctions. I then present micro-evidence for an increase of DoS attacks after the imposition of sanctions against Russia in 2014, before I discuss the method and results of the macro-analysis.

Emotions, Sanctions, and DoS Attacks

Following studies from social identity theory (Tajfel 1978) and their application to international relations (e.g., Sasley 2011; Larson and Shevchenko 2014), aggressive foreign policy events can influence the political behavior and emotions of states, various groups within the country, and society at large. Foreign policies such as sanctions may be perceived as humiliating, trigger anger, and increase hostility against the foreign aggressor (see Sasley 2011).

The Internet has provided new disruptive ways for states and individuals to show this anger and displeasure. DoS attacks have some useful properties as a retaliation tool in this regard. First, they are hard to trace back, making it a relatively low risk to use them. Second, DoS attacks are brute force and easy to conduct. Perpetrators do not have to rely on sophisticated tools and infrastructure to launch these attacks.[3] Nonetheless, if DoS attacks are successful in disabling the targeted servers, they are still visible and can lead to considerable economic costs. Cybersecurity firms speak of around 40,000 US dollars per hour when business websites are taken offline (Matthews 2014).

On the one hand, governments or government-related entities targeted by sanctions may use DoS attacks to retaliate and display displeasure. Governments can either rent botnets themselves or "order" own cyber groups to launch these attacks. Since the ultimate attribution of DoS attacks remains difficult, their use comes with minimal costs; i.e., a physical or digital retaliation to these attacks is unlikely (Valeriano, Jensen, and Maness 2018).

On the other hand, the simplicity of DoS attacks enables not only governments but also citizens and patriotic hacker groups to respond in this fashion. Sanctions reinforce nationalist sentiments and make citizens more susceptible to government propaganda (Galtung 1967). These nationalist sentiments likely increase hostility against the sender country (Grossman, Manekin, and Margalit 2018), and may even encourage citizens to engage in collective action in favor of the government (Hellmeier 2020), including the use of politically motivated cyberattacks to do so (Holt et al. 2017).

2 Although I focus on sanctions in this paper, the results may likely be comparable to other aggressive foreign policies, e.g., trade wars or kinetic conflict.

3 This is different for so-called advanced persistent threats, state-sponsored groups that launch custom-tailored cyberattacks and that require highly sophisticated infrastructure (Geers et al. 2014).

In their analysis of the use of DoS attacks during the Russo-Georgian War in 2008, Deibert, Rohozinski, and Crete-Nishihata (2012) show that it was very plausibly Russian citizens, groups, and hackers who were responsible for the large-scale DoS attacks during the conflict. A similar conclusion is made by Rid (2012) who investigates the 2007 DoS attacks against the Estonian government, news, and industry websites. These large-scale attacks happened after the Estonian government relocated a Soviet Union memorial site in disagreement with the Russian government. Although many pundits describe this incident as a government-planned act of cyber warfare, there is evidence that many citizens and pro-government hacking groups just wanted to show disapproval (Ottis 2008). Likewise, Kostyuk and Zhukov (2019) do not find strong support for a strategic use and interaction between DoS attacks and battlefield events during the ongoing civil conflicts in Ukraine and Syria.

As it nevertheless remains difficult to attribute cyber operations, governments may have been actively involved during these incidents as well. Besides, governments likely facilitate the use of DoS attacks by citizens and non-state groups due to their use of propaganda to take action against foreign aggression, as well as their sponsoring of patriotic hacking groups. Finally, since one can start DoS attacks globally, not only domestic citizens but also activists worldwide who disagree with a government's policy may use these attacks (see Lutscher et al. 2020).

To summarize, when states, groups, or individuals indeed use DoS attacks to retaliate digitally, we should expect that aggressive foreign policies increase the frequency of DoS attacks against the sender state. Related to sanction events that means, first, that

H1: *The frequency of DoS attacks rises against the sender state when it threatens sanctions.*

Second, this increase should be stronger when states impose sanctions as this policy is more salient and should fuel negative sentiments toward the sender state more strongly (Galtung 1967). We should thus expect that

H2: *The frequency of DoS attacks rises against the sender state when it imposes sanctions and this increase is stronger compared to sanction threats.*

An alternative explanation would be that states use DoS attacks strategically in response to sanction events in order to gain concessions, i.e., the lifting or non-imposition of sanctions. Previous theoretical (e.g., Gartzke 2013) and empirical (e.g., Valeriano, Jensen, and Maness 2018) studies find little evidence for such a coercive use of cyber operations. In particular for DoS attacks, it is questionable how these actions should influence foreign policy decisions and be perceived as a credible threat. As described above, DoS attacks are hard to attribute, and—compared to other more advanced cyber operations—they only come with limited costs, which makes it difficult to perceive them as a costly signal.

Data

Data on DoS Attacks

The main data for this study comes from the Center for Applied Internet Data Analysis (CAIDA) at the University of California, San Diego from 2008 to 2016 (CAIDA 2016). CAIDA measures DoS attacks 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. CAIDA can measure these attacks because attacked servers still respond to requests made by the *fake* IP address of the attacker and this response may end up within a large address space of unassigned IPv4 addresses monitored by CAIDA (see Moore et al. 2006, for more technical details).[4] Compared to previous media-based approaches, this measurement approach is by construction not prone to media biases, neither media attention nor underreporting 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. Regarding the latter, media outlets likely miss to report a large share of cyber incidents, either because they are not observed (Poznansky and Perkoski 2018) or because they are simply not newsworthy (Earl et al. 2004). The data by CAIDA can get a more comprehensive picture of DoS attacks worldwide. The data include information about attack strength and duration, the timing of the attack, and the targeted IP address. In this paper, I use this information to retrieve the number of spoofed DoS attacks per country and day from March 2008 until December 2015. More precisely, I rely mainly on attack data against servers hosted in the United States and the EU for which I summed up DoS attacks against each member state.

Despite these advantages, the data come with some limitations (Moore et al. 2006). First, CAIDA captures a subset of DoS attacks. The measurement is thus an approximation for the overall level of DoS attacks. Even so, recent studies show that spoofed DoS attacks are comparable to other popular DoS attack vectors (Jonker et al. 2017). Second, since attackers use fake addresses, I

4 The monitored space is approximately 1/256th of all unassigned IPv4 Internet addresses.

cannot infer the identity of the attacker or even the attack's country of origin but have information on the targeted country only. However, even if newspapers may report on potential perpetrators, this information is often not reliable because attackers use botnets, spoofing methods, and other techniques to hide their true identities.

Data on Sanction Events

The EUSANCT dataset is the second main data source I use in this paper (Weber and Schneider 2020). The dataset extends and merges previous sanction datasets (e.g., Morgan, Bapat, and Kobayashi 2014), and contains information on sanction episodes from 1989 until the end of 2015 for the three most important sanction senders, the United States, the EU, and the United Nations (UN).

In defining sanction episodes, threats, and impositions, Weber and Schneider (2020) closely follow the TIES dataset (Morgan, Bapat, and Kobayashi 2014). A sanction episode normally starts with a sanction threat, which is defined as a verbal statement of government officials, drafting of legislation against a target state, or conditional laws, stating that sanctions are a possibility against a target state if certain target behaviors do not change. Sanction impositions are then the formal realizations of these threats.

From March 2008 until December 2015, the data record 29 or 20 sanction threats and 28 or 23 impositions by the United States or the EU, respectively. I do not focus on UN sanctions because it would be difficult to determine where to expect an increase in DoS attacks.[5]

Case Evidence: The Crimean Crisis in 2014

In a first step, I use both data sources to investigate one of the likeliest cases for which one should expect to find evidence: sanctions against Russia in 2014.[6] 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 Unites States imposed the first set of sanctions on March 6, which included travel bans and the freezing of US assets for several 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 EU undertook similar actions and imposed visa restrictions and froze assets. On March 18, Russia annexed the Crimean Peninsula. Around the same dates, the governments of Canada, Australia, New Zealand, and Japan imposed sanctions against Russia as well.

Figure 1 shows the number of DoS attacks against servers hosted in the United States and the EU. The top panel reveals that attacks against the United States peaked eleven days after the United States imposed their first set of sanctions. 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 data record an increase in DoS attacks against the EU with the highest number of DoS attacks on the imposition date (bottom panel). Looking at the other sanctioning countries supports this finding (see figure 2). In particular, the number of DoS attacks against Canada spiked when the country imposed sanctions and for Australia when the country supported the Security Council resolution by the United States. Moreover, figure A1 in online appendix A illustrates that DoS attacks against servers hosted in Russia and Ukraine increased during the same period, suggesting a kind of "digital clash" between both countries.

What can be said about the motivation and potential perpetrators in this case? First, botnet activities originating from Russia and Ukraine increased during this period, suggesting that Russian botnets were used to launch DoS attacks (Gilbert 2019). Second, news outlets reported about DoS attacks against several NATO websites on March 16 by a group named Cyber Berkut. This group emerged in 2014 as a Ukrainian pro-Russian hacktivist group (Cherney 2014). Third, an own Google trend investigation of the term "denial-of-service attack" shows a remarkable increase in interest in the technique in Russia. 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 3 shows that the trend gained momentum after the imposition of the US sanction, especially just

5 For the later macro-analysis, the variable remains binary for the few imposition or threat dates on which several sanctions were imposed or threatened. In five cases for the United States, and two cases for the EU, sanction impositions and threats overlap on the same day.

6 In online appendix A, I explore two other high-profile cases, sanctions against Iran in 2010 and Syria in 2011, similarly finding an increase of DoS attacks after sanction impositions, in particular against servers hosted in the United States.

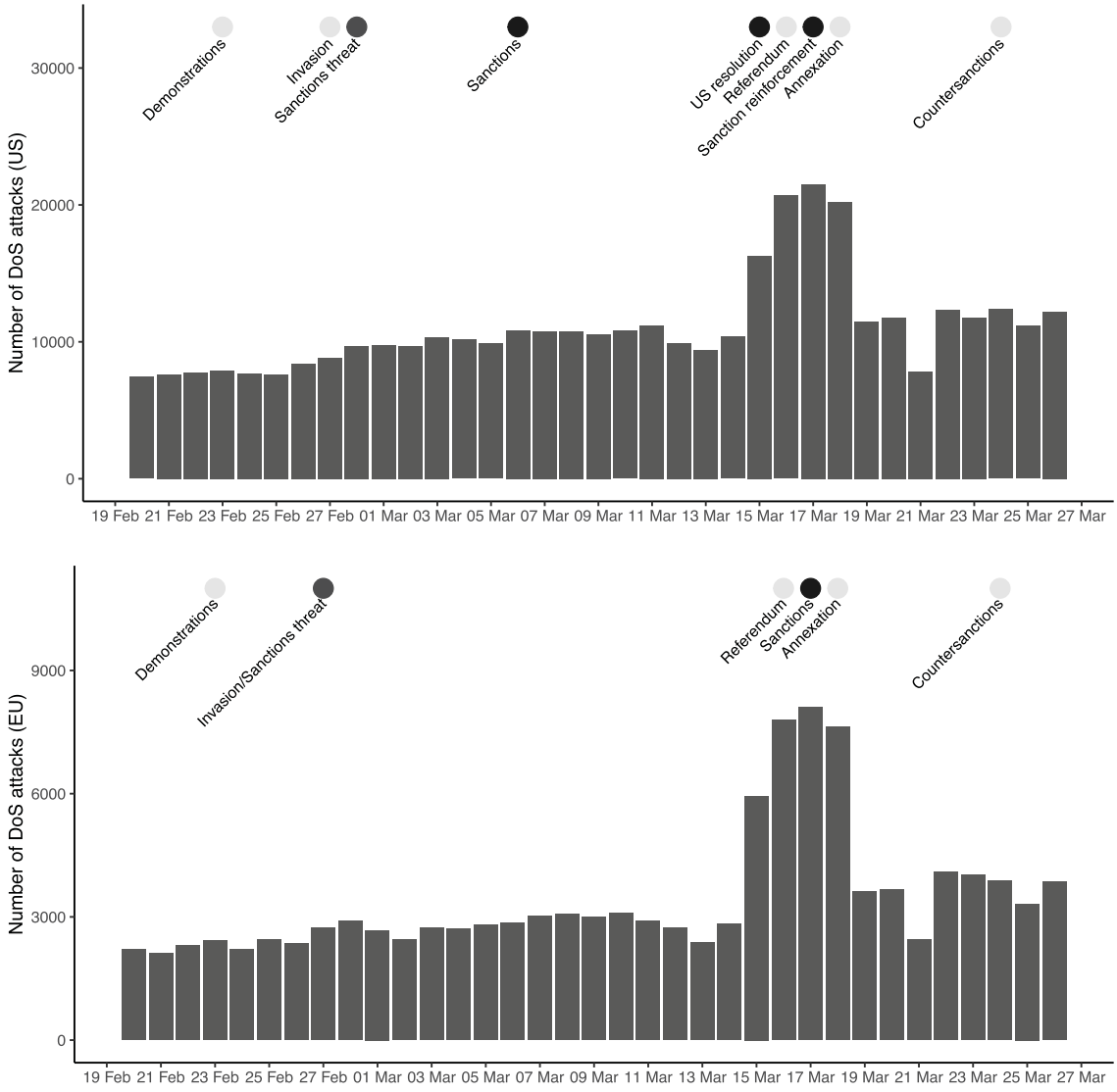

Figure 1. Number of DoS attacks in the United States and the EU (February/March 2014).
Note: Development of DoS attacks (vertical bars), sanction-related events (black dots), threats (dark gray dots), and other events (gray dots).

before the referendum weekend, and displays overall high correlations to the development of DoS attacks against the United States and the EU in figure 1 ($r = 0.56$ and $r = 0.51$, respectively). 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.[7] Although this does not allow to make any causal claims as media coverage on DoS attacks or some other factor may influence search queries as well, it is worthwhile mentioning that interest spiked *before* the rise in DoS attacks. Finally, Frye (2019) shows in survey experiments that the annexation of Crimea increased citizens' support for the Russian government.

It appears therefore overall plausible that some citizens displayed their increased anger against the United States and the EU by using DoS attacks. Nevertheless, while 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

7 As this term is more volatile, a systematic investigation remains challenging. Moreover, although Google is not the main search engine in Russia, I believe that this should not alter its use as a proxy for public interest.

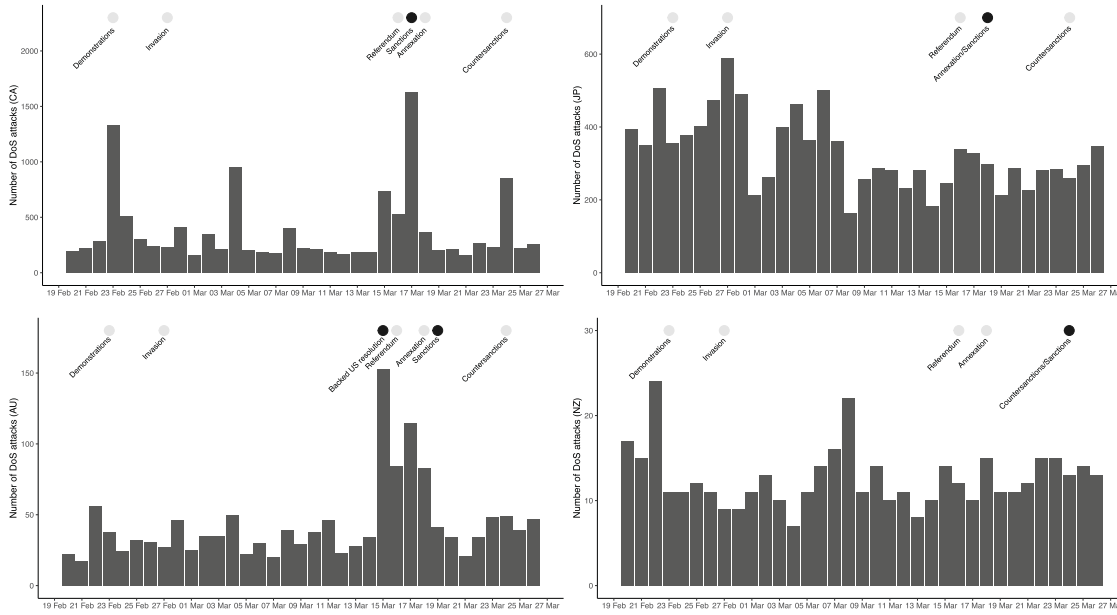

Figure 2. Other sanctioning states (February/March 2014).

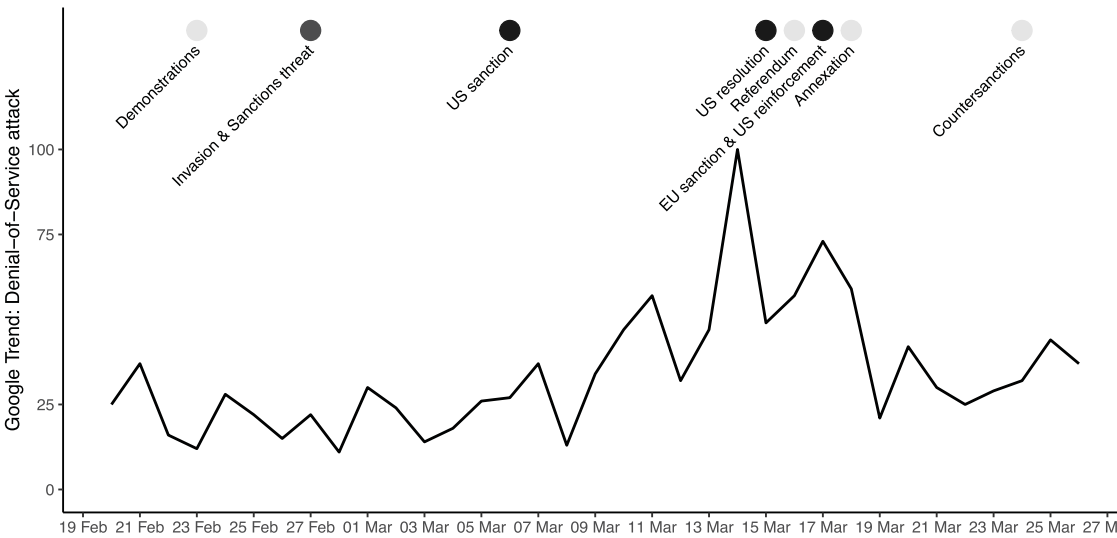

Figure 3. Russian Google trend for DoS attack (February/March 2014).

Crete-Nishihata 2012), it may still be that government entities used DoS attacks to retaliate in this fashion as well.[8]

An alternative explanation for the increase in DoS attacks against the United States and the EU could be that perpetrators launched DoS attacks against servers that host Ukrainian websites in the United States or the

8 To be clear, I do not argue that the Russian government is not conducting cyber actions. In fact, there is evidence that the Russian intelligence services are responsible for many cyber operations that involve espionage and infiltration campaigns worldwide. However, in contrast to DoS attacks, these operations require much more resources and planning ahead of time.

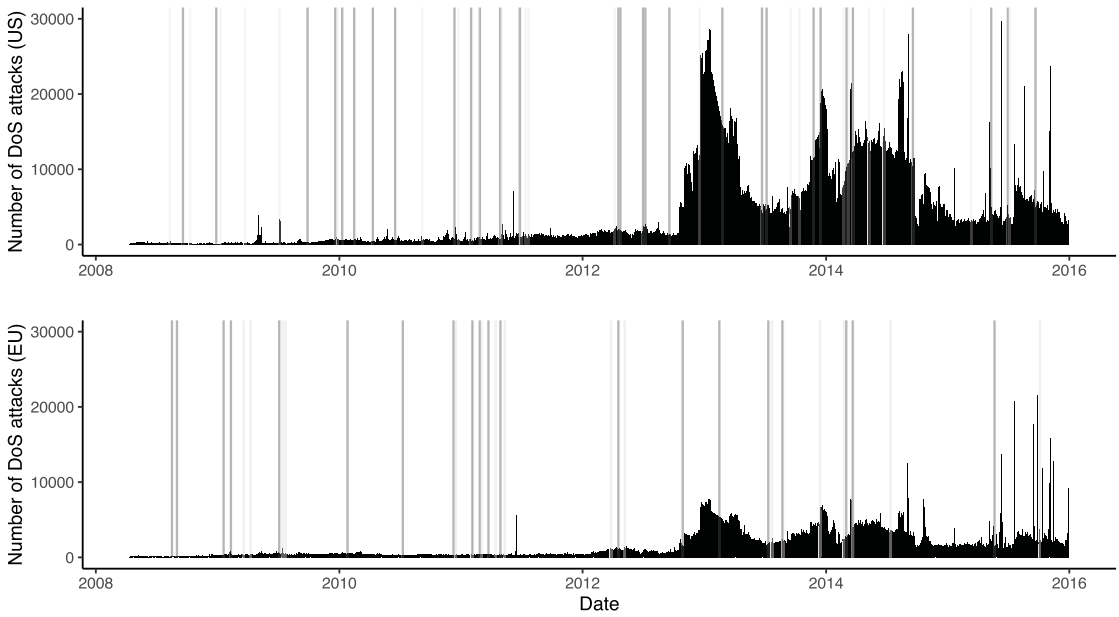

Figure 4. Number of DoS attacks against the United States and the EU, sanction threats (light gray), and sanction impositions (dark gray).

EU (see Lutscher et al. 2020). Although this was also likely the case, the increasing number of DoS attacks on other sanctioning countries and the presented anecdotal evidence support the conclusion that US- and EU-related servers suffered from DoS attacks as well.

Macro-Evidence: US and EU Sanctions

To investigate whether the findings from the case study hold more broadly, I combined the DoS and sanction data for the most important sanction senders—the United States and the EU. Figure 4 illustrates the created daily time series from 2008 until the beginning of 2016. Afterward, I run so-called autoregressive distributed lag models that can model short- and long-term temporal relationships between variables (Hendry 1995; Philips 2018). These linear regression models allow to include a sufficient number of lags for both the independent, sanction threats and impositions, and the dependent variables, the number of DoS attacks against the United States and the EU.

To run these models reliably, I had to pre-process and transform the data. More precisely, I analyze changes in the normalized number of DoS attacks for two distinct periods that last from March 2008 until February 2012 and again from February 2012 until December 2015. Finally, I followed the literature and used the Akaike information criterion to determine the best fitting number of lags to include in the models (Burnham and Anderson 2004). The pre-processing steps and method are explained in detail in online appendix B.

In the presentation of the results, I follow recent approaches and simulate counterfactual scenarios for variables of interest (Philips 2018).[9] For the simulation of the development of DoS attacks displayed in figure 5, I set a hypothetical sanction imposition to the point in time "5" (dashed vertical line) and assume that there is no sanction threat. The dashed horizontal line shows the null effect that is the value for which the non-normalized change in the number of DoS attacks is zero.

The figure shows that in all simulations the 90 and 95 percent confidence intervals cross the horizontal line (null effect) for all points in time. The results thus do not suggest any significant increase in DoS attacks after the imposition of sanctions. As shown in online appendix C, simulations for sanction threats also display a null and even no temporal effects.[10] Does this mean that the case

9 In online appendix C, I report the full regression models and long-run multiplier coefficients.

10 A caveat may be that within sanction periods the sender state(s) reinforce threats and the severity of the sanction gradually that could influence the decision to retaliate digitally. Unfortunately, this information is not

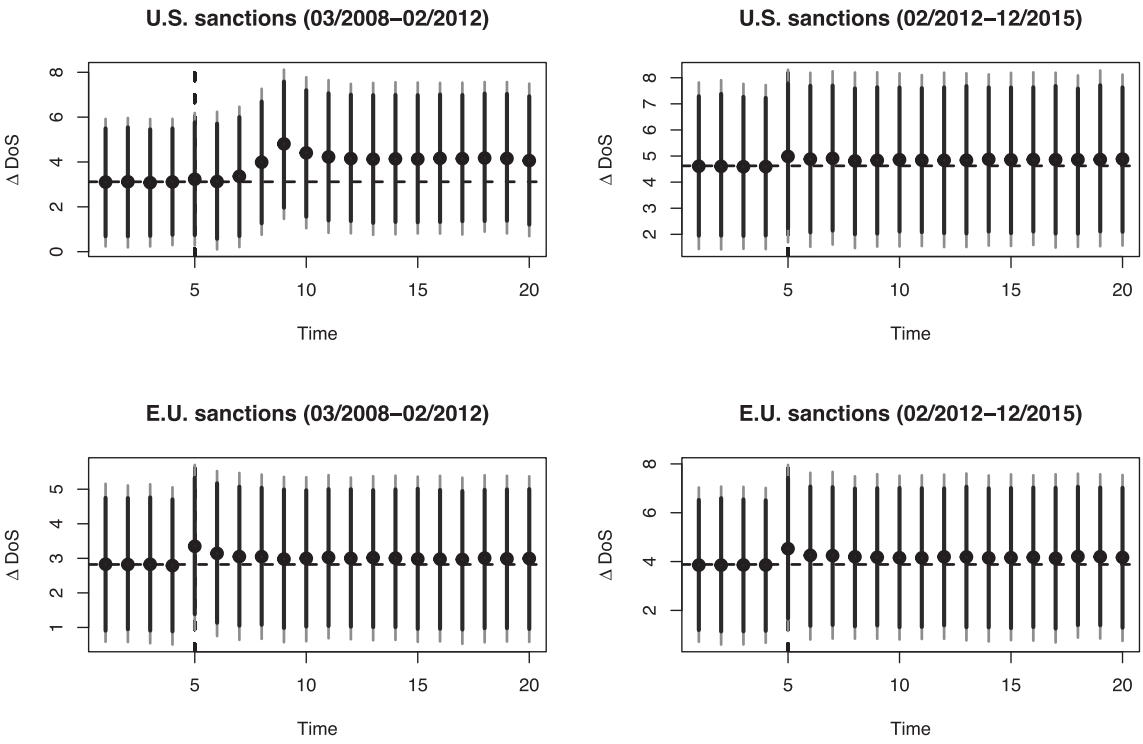

Figure 5. Simulations of DoS attacks.
Note: Based on 10,000 draws; 95 and 90 percent confidence intervals are displayed. The intervention is marked with a dashed vertical line, while the horizontal line shows the null effect. The US and EU time series are split at their respective breaking points.

study from above is an exception? Or does Russia have specific properties that make a digital retaliation more likely?

It is well known that Russia is an active player in cyberspace, possesses sufficient cyber capabilities, and has active patriotic hacking groups. Although DoS attacks are relatively simple to conduct, using them at large requires a certain level of technological advancement, making it worthwhile to investigate the impact of sanctions conditional on this factor. To measure technological advancement comparatively, I rely on a proxy variable and use the information and communication technology (ICT) development index (IDI) by the International Telecommunication Union (ITU). This variable measures the access to, use of, and skills regarding modern ICTs for countries worldwide (ITU 2017).[11]

Figure 6 illustrates the results when I exclusively consider sanctions against countries that score 25 percent or above in the IDI compared to the yearly worldwide average.[12] The results indeed change. In particular for the US time series for the time period later than February 2012, the simulation displays a steady increase of DoS attacks, with a peak at day 11 after the imposition date, where the 90 percent confidence intervals of the simulated change in the number of DoS attacks are clearly distinguishable from the horizontal dashed line (null effect). Since the substantial predictions of the normalized models are hard to interpret, I run non-normalized models that are reported in online appendix D. These models illustrate similar patterns and predict a maximal

available in Weber and Schneider (2020). Nevertheless, it is fair to assume that if states and/or groups within states use DoS attacks to retaliate, we should already expect this happening after the first serious threat and/or imposition.

11 Since the ITU does not publish the IDI every year, I fill values for years in between using linear imputation.

12 When using this threshold, the number of considered sanction impositions decreases to 11 and 10 for the United States and the EU, respectively.

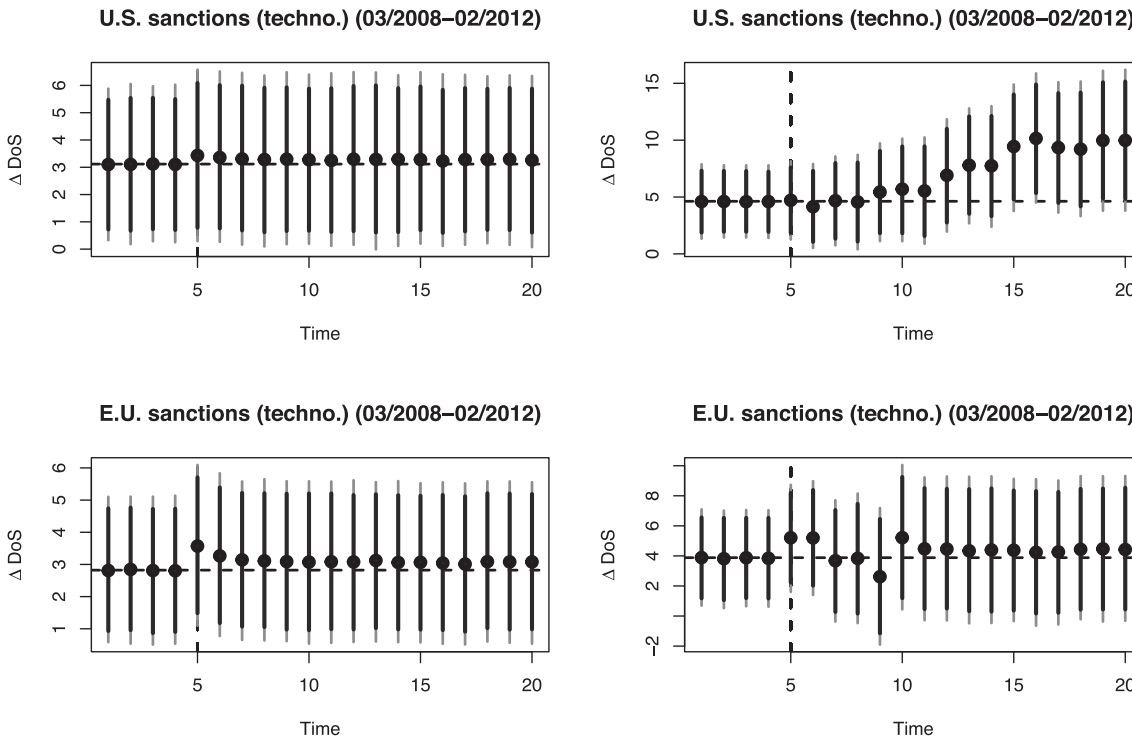

Figure 6. Simulations of DoS attacks exclusively considering sanctions on technologically advanced countries.

increase of approximately 5,000 DoS attacks against US servers after the imposition of sanctions.[13]

Furthermore, as detailed in the same supplementary material, I show that this increase becomes even stronger when using 50 or 75 percent as thresholds to define technologically advanced countries. Moreover, the results remain similar when using another index to measure cyber capabilities proposed by Valeriano, Jensen, and Maness (2018). For sanction threats, in contrast, the simulations still suggest a null finding regardless of the targeted country's technological advancement (see online appendix C for details).

To further explore how valid these findings are, I conduct additional sensitivity and robustness tests that are reported in online appendix D. These tests include Granger tests, placebo tests, different operationalizations for the dependent and independent variables, and different model specifications. In sum, most of the additional models support the finding of a positive correlation between sanction impositions and the number of DoS attacks against the United States when the targeted country is sufficiently technologically advanced. However, two caveats remain. First, placebo tests using GDP per capita to measure technological advancement show similar results, suggesting that not necessarily a country's technological advancement but general economic development is important in increasing the number of DoS attacks. However, since both variables highly correlate ($r = 0.9$), it is difficult to distinguish both concepts. Second, some of the additional models indicate that specific sanctioning cases, foremost the Russian one, can be seen as an influential observation in the statistical analysis. Leaving out the Russian case still shows similar patterns, yet, with slightly higher levels of uncertainty.

13 Another solution would be to transform the predictions of the, statistically more appropriate, normalized models. However, while these models allow drawing robust inference, such back-transformed predictions are imprecise, suggesting a maximal increase of approximately 37,000 DoS attacks.

Conclusion

Using data on DoS attacks inferred from Internet data traffic, this study investigated the use of DoS attacks against sanction sender states. While my study could find no evidence for an increase of DoS attacks when countries *threaten* sanctions, my results point to a digital

retaliation when countries *impose* sanctions. Nevertheless, such a use seems to be conditional on one factor: the sanctioned country needs a certain level of technological advancement or development.

One main problem in studying cyberattacks remains their attribution. I thus cannot make definite claims about the perpetrators and motivation of the measured DoS attacks. My case study on Russia suggests that it had been likely patriotic groups and individuals launching DoS attacks against servers in the United States and the EU to signal displeasure. While some cyber conflict studies argue that states use cyberattacks also as a strategic tool to gain concessions (e.g., Sharp 2017), my study shows that for DoS attacks this seems rather unlikely the case. The frequency of attacks spiked for a short period only, and their effects and overall costs appear to be still limited (cf. Rid 2012; Gartzke 2013).

Finally, this research innovation advances the empirical cyber conflict literature (e.g., Valeriano and Maness 2014; Asal et al. 2016; Valeriano, Jensen, and Maness 2018). Whereas previous work likely suffered from media biases, either under- or overreporting, the data used in this paper enable researchers and the public to get a more comprehensive picture of cyber activities worldwide. Future research may use these data to investigate similar questions such as cyber conflict dynamics (e.g., Kostyuk and Zhukov 2019) or how domestic events influence DoS attacks (e.g., Lutscher et al. 2020).

Acknowledgments

I would like to thank Nils Weidmann, Molly Roberts, and Karsten Donnay for their support and valuable comments from early stages of this project. Furthermore, I thank Sebastian Hellmeier, Anita Gohdes, Lukas Kawerau, Patrick Weber, Eda Keremoglu, Julian Schüssler, and Max Heermann who helped a lot in improving this paper. Finally, I thank the two anonymous reviewers and the editors of the JOGSS, whose comments led to major improvements of this paper. All remaining errors are my own.

Supplementary Information

Replication material is available at the author's OSF data archive: https://osf.io/rxez8.

Conflict of interest

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

Funding

Work for this project was supported by the DFG grant 402127652 and by the National Science Foundation grant CNS-1730661. This material is based on research sponsored by the Air Force Research Laboratory under agreement number FA8750-18-2-0049. The US Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the US Government. This work used the Extreme Science and Engineering Discovery Environment (XSEDE), which is supported by the National Science Foundation grant number ACI-1053575.

References

Asal, Victor, Jacob Mauslein, Amanda Murdie, Joseph Young, Ken Cousins, and Chris Bronk. 2016. "Repression, Education, and Politically Motivated Cyberattacks." *Journal of Global Security Studies* 1 (3): 235–47.

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

CAIDA. 2016. "The CAIDA UCSD Near-Real-Time Network Telescope: 2008–2016." CAIDA, UC San Diego. Accessed January 21, 2021. https://www.caida.org/data/passive/telescope-near-real-time_dataset.xml.

Cherney, Max. 2014. "Pro-Russian Hackers Took Down Three NATO Websites. The Work of Russian Cyber-Agent Provocateurs?" *Motherboard*, March 16. Accessed July 29, 2019. https://motherboard.vice.com/en us/article/jp5mxd/pro-russia-ukranians-hack-nato-websites.

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.

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.

Frye, Timothy. 2019. "Economic Sanctions and Public Opinion: Survey Experiments from Russia." *Comparative Political Studies* 52 (7): 967–94.

Galtung, Johan. 1967. "On the Effects of International Economic Sanctions, with Examples from the Case of Rhodesia." *World Politics* 19 (3): 378–416.

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

Geers, Kenneth, Darien Kindlund, Ned Moran, and Rob Rachwald. 2014. "WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks." *FireEye*.

Accessed June 28, 2019. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf.

Gilbert, David. 2019. "Inside the Massive Cyber War between Russia and Ukraine." *Vice*, March 29. Accessed July 29, 2019. https://news.vice.com/en_us/article/bjqe8m/inside-the-massive-_cyber-war-between-russia-and-ukraine.

Grossman, Guy, Devorah Manekin, and Yotam Margalit. 2018. "How Sanctions Affect Public Opinion in Target Countries: Experimental Evidence from Israel." *Comparative Political Studies* 51 (14): 1823–57.

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* 100 (4): 817–85.

Hellmeier, Sebastian. 2020. "How Foreign Pressure Affects Mass Mobilization in Favor of Authoritarian Regimes." *European Journal of International Relations*. doi:10.1177/1354066120934527.

Hendry, David F. 1995. *Dynamic Econometrics*. Oxford: Oxford University Press.

Holt, Thomas J., Max Kilger, Lichun Chiang, and Chu-Sing Yang. 2017. "Exploring the Correlates of Individual Willingness to Engage in Ideologically Motivated Cyberattacks." *Deviant Behavior* 38 (3): 356–73.

International Communication Union (ITU). 2017. "The ICT Development Index (IDI): Conceptual Framework and Methodology." Accessed January 21, 2021. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx.

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)*, 100–113. New York: ACM.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63 (2): 317–47.

Larson, Deborah Welch, and Alexei Shevchenko. 2014. "Russia Says No: Power, Status, and Emotions in Foreign Policy." *Communist and Post-Communist Studies* 47 (3–4): 269–79.

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 (1–2): 1–29.

Matthews, Tim. 2014. "Incapsula Survey: What DDoS Attacks Really Cost Businesses." *Incapsula*. Accessed July 29, 2019. https://lp.incapsula.com/rs/incapsulainc/images/eBook20-20DDoS20Impac20Survey.pdf.

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* 24 (2): 115–39.

Morgan, T. Clifton, Navin Bapat, and Yoshiharu Kobayashi. 2014. "Threat and Imposition of Economic Sanctions 1945–2005: Updating the TIES Dataset." *Conflict Management and Peace Science* 31 (5): 541–58.

Ottis, Rain. 2008. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. In *Proceedings of the 7th European Conference on Information Warfare*, 163–69.

Pagliery, Jose. 2018. "U.S. Banks Prepare for Iranian Cyberattacks as Retaliation for Sanctions." Accessed July 30, 2019. https://edition.cnn.com/2018/11/09/tech/iran-sanctions-us-banks-cyber-hack-invs/index.html.

Perlroth, Nicole, and Quentin Hardy. 2013. "Bank Hacking Was the Work of Iranians, Officials Say." Accessed July 30, 2019. https://www.nytimes.com/2013/01/09/technology/online-banking-_attacks-were-work-of-iran-us-officials-say.html.

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): 230–44.

Poznansky, Michael, and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3 (4): 402–16.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32.

Sasley, Brent E. 2011. "Theorizing States Emotions." *International Studies Review* 13 (3): 452–76.

Sharp, Travis. 2017. "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony." *Journal of Strategic Studies* 40 (7): 898–926.

Tajfel, Henri, ed. 1978. *Differentiation between Social Groups: Studies in the Social Psychology of Intergroup Relations*. London: Academic Press.

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): 347–60.

Weber, Patrick M., and Gerald Schneider. 2020. "Post-Cold War Sanctioning by the EU, the UN, and the US: Introducing the EUSANCT Dataset." *Conflict Management and Peace Science*. doi:10.1177/0738894220948729.