Journal of Peace Research

Pulling the plug: Network disruptions and violence in civil conflict

Journal of Peace Research
2015, Vol. 52(3) 352–367

DOI: 10.1177/0022343314551398
jpr.sagepub.com
SAGE

Anita R Gohdes

School of Social Sciences, University of Mannheim

Abstract

New media outlets have been deemed a vital instrument for protesters and opposition groups to coordinate activities in the recent civilian uprisings in the Middle East and North Africa. But what happens when regimes respond by shutting down the internet? I argue that governments have a strategic incentive to implement internet blackouts in conjunction with larger repressive operations against violent opposition forces. Short-term intermissions in communication channels are expected to decrease opposition groups' capabilities to successfully coordinate and implement attacks against the state, allowing regime forces to strengthen their position. Network blackouts should consequently be accompanied by significant increases in military activity. Analyzing daily documented killings by the government in the Syrian civil war, I find that blackouts occur in conjunction with significantly higher levels of state repression, most notably in areas where government forces are actively fighting violent opposition groups. In addition, I estimate the number of undocumented conflict fatalities prior to and during network blackouts to test whether they are implemented to hide atrocities from outside observers, and find no support for this hypothesis. The results indicate that such network blackouts constitute a part of the military's strategy to target and weaken opposition groups, where the underreporting of violence is not systematically linked to outages.

Keywords

censorship, internet disruption, new media, repression, Syria, violence

> We fear what we will find when the internet is switched back on. #Syria[1]

Introduction

The civil war in Syria presents the first case of large-scale civil conflict that has been painstakingly captured, documented, and communicated via the internet. Thousands of YouTube videos record the images of killed and injured people in morgues, hospitals, and market places, and activists within and outside the country use countless Twitter and Facebook accounts to inform each other about military operations and massacres, and to organize and coordinate the revolution (Youmans & York, 2012). The Syrian government has equally acknowledged the importance of upholding a strong virtual presence, and employs a Syrian Electronic Army to spread the regime's message throughout the virtual world. Under the banner of the 'Syrian Presidency', President Bashar Al-Assad even maintains a lively Instagram account with no discernible sign of the ongoing war.[2] On a number of occasions, however, the internet connection has been completely cut for periods between an hour and three days. Evidence on the trajectory of these outages suggests that technical failures as the possible cause can be ruled out (Gallagher, 2012).

Recent research has focused on the potential new technologies offer to opposition movements (Diamond, 2010). The logic and effect of these technologies being

[1] Lina Sergie Attar, journalist, on Twitter, 29 November 2012: https://twitter.com/AmalHanano/status/274169153781387265.

[2] See http://instagram.com/syrianpresidency.

Corresponding author:
anita.gohdes@uni-mannheim.de

temporarily shut down, however, remains largely unclear. The fact that Syria is currently fighting 'the most socially mediated civil conflict in history' (Lynch, Freelon & Aday, 2014: 5) indicates the crucial role the internet is likely to play in future conflicts. Understanding the motivation behind network manipulations instituted by regimes fearful of their political demise is therefore becoming increasingly important for our theoretical and practical understanding of conflict dynamics. Learning from current cases such as Syria is an important place to start.

In this article, I argue that governments fighting to maintain political control have an incentive to implement internet blackouts in conjunction with larger military offensives aimed at restoring control. Regime forces are likely to utilize these shutdowns as a tactical advantage when facing intense confrontation from violent opposition groups. The reduced opportunities for short-term military coordination of attacks is expected to improve government-aligned fighters' chances of regaining control previously challenged by antigovernment fighters. If the shutdown of all communication networks is implemented when repressively responding to increased resistance, regime forces are likely to be involved in increased fighting, directly prior to and during the period of the outage. One observable consequence is therefore constituted by an increase in violence perpetrated by regime supporters immediately prior to and during such outages.

I empirically test this proposition using new data on reported daily incidences of fatal regime violence between March 2011 and September 2013 that links the information collected by five human rights groups working in Syria. I find that government-induced network blackouts are accompanied by significantly higher levels of violence, in particular in the governorates where government and opposition forces are directly confronting each other.

An alternative explanation is that governments do not anticipate operational advantages by cutting connections, but instead implement blackouts to commit atrocities that are hidden from international scrutiny. To test for this cover-up hypothesis, I use log-linear capture-recapture models to estimate the degree of underreporting of conflict fatalities during blackouts, and compare them to the already existing levels of underreporting on days prior to network outages. The evidence suggests that unreported violence does not systematically increase during network outages, which is most likely attributable to the very short disruption intervals. Instead, the increase in documented violence indicates that network outages are likely to form a part of the Syrian regime's coercive response strategy.

The next two sections review recent research on censorship and blocking of the internet as well as the relationship between network accessibility and the potential for conflict. I then discuss the theoretical motivations and potential costs for governments to disrupt network services when being challenged by armed opposition groups. Following a discussion of possible alternative motivations, I formulate empirical expectations that can be tested to uncover the predominant motivation behind implementing outages. The empirical section introduces the data on regime violence and network outages in Syria, and then proceeds to present the results of the analysis of documented violence, and the variation in documentation patterns during outages. The article concludes with a discussion of the results and potential avenues for future research.

Recent research on censorship in the internet age

Although the recent popular uprisings in the Middle East and North Africa have garnered a lot of attention for the role of the 'New Media' in organizing protest and rebellion (Breuer, Landman & Farquhar, forthcoming; Howard & Hussain, 2011; Tufecki & Wilson, 2012), less is known about how regimes facing such status quo challenges use these new technologies to their own advantage. Case evidence indicates that incumbent regimes try to limit the potential for collective organization via the internet by manipulating and censoring information. For example, during the 2009 uprising, the Iranian government allegedly disrupted internet access in the immediate aftermath of the elections, and furthermore, SMS text-messaging was blocked during the entire election period (Aday, Farrell & Lynch, 2010: 20–21).

Shutting down internet and cell phone services can be understood as an extreme form of government censorship against a country's own population (Deibert, 2008). Howard, Agarwal & Hussain (2011) document 556 network outages between 1995 and 2011 across the world, with half of them occurring in authoritarian regimes. Their analysis suggests that while democratic governments generally shut down internet access in an attempt to combat child pornography, authoritarian regimes use it in response to perceived national security issues, such as social and political unrest (Howard, Agarwal & Hussain, 2011: 225). More recent examples of this process can be found in Libya and Egypt, where the internet was cut off in response to antigovernment

demonstrations in 2011 in both countries (Edmond, 2011). In September 2013, in the midst of antigovernment protests sparked over fuel prices, Sudan responded by disconnecting its citizens from the internet (Madory, 2013), and the Central African Republic witnessed brief intermissions of all internet connections in the midst of ongoing violent clashes in December 2013. Burma's regime shut off all connections in response to the Monks' protests in 2008, and China proceeded to take its Xinjiang province offline during ethnic riots in 2009 (MacKinnon, 2012: 51). Evidently, the current Syrian regime is not the first to make use of this method in the wake of persistent rebellion and protests.

What remains unclear is to what extent network shutdowns are implemented as part of a military response to violently repress opposition groups, or whether they constitute a mere attempt to limit reputation damage by stopping the outside world from following events on the ground. In this article, I argue that in situations of civil conflict, temporary network outages are used as part of a response tactic aimed at gaining an advantage over the opposition in larger, short-term operations of repression, rather than as a means of concealing atrocities from international scrutiny.

Network accessibility, repression, and conflict

Repressive governments have a long history of using nuanced, proactive methods of censoring online content that is deemed hazardous to maintaining their status quo (see MacKinnon, 2012). Deibert & Rohozinski (2010) distinguish between three generations of internet control, where the first generation presents the most primitive form of blocking content, and the second and third generations involve more subtle ways of warrantless surveillance and normative campaigns against critical information. Analyzing the modes of control in Russia and the Commonwealth of Independent States, they find that highly authoritarian states are more likely to use traditional content-blocking to censor their cyberspace, whereas more democratic countries opt for less intrusive, surveillance-based approaches. The authors argue that the regimes still implementing full disruptions are also those most afraid of their control being challenged through online protest mobilization (Deibert & Rohozinski, 2010: 28–29).

The risk of virtual communication inciting political unrest is corroborated by the behavior of other nondemocratic governments, the largest being China. In a large-scale quantitative analysis of social media censorship, King, Pan & Roberts (2013) find that censoring in China is only aimed at comments and posts that could motivate collective action or advance the coordination of protests. In contrast, comments critiquing the government or its policies are not censored as they are not deemed threatening to the status quo. The level of sophistication involved in capturing and removing these specific comments suggests that the Chinese government perceives action-inciting comments as an actual threat to the regime's stability.

Recent research examining the effect of increased access to new technologies on collectively organized violence indicates that the Chinese government's fear might not be unwarranted: analyzing cell phone coverage across African countries, Pierskalla & Hollenbach (2013) find that locations with better access to wireless phone networks display higher numbers of violent events.[3] Taking a closer look at the insurgent side of internal conflict, the authors argue that cohesive rebellious activities are a challenge to coordinate – especially when groups are secretly operating across different locations – and therefore strongly benefit from the availability of cheap communication tools (Pierskalla & Hollenbach, 2013: 210).

In contrast, Shapiro & Weidmann (2015) argue that from the position of governments, increased networking opportunities also increase the possibility of civilians unwittingly sharing knowledge about planned opposition attacks with state forces, thus throttling rebellious actions. Analyzing cell phone usage in the Iraqi conflict, they find that insurgent violence is significantly lower where increased mobile communication is available. These two contradictory findings indicate the variable potential of decentralized communication on conflict, which might depend on whether the majority of a local civilian population supports the opposition or the regime.[4]

From the position of the government, the availability of cell phone and internet connections can therefore be boon and bane, providing both intelligence against the opposition and a space for coordination of the opposition at the same time. The next section examines when and why a temporary cut of all internet services can be a rational policy option for governments who see their status quo threatened.

[3] Shapiro & Weidmann (2015) highlight a potential weakness: violent events are also more likely to be reported where communication is facilitated by mobile networks.

[4] Maintaining a neutral position in the face of conflict cleavages can pose a higher risk than taking a side, and in the face of increased communication flows on the ground, staying neutral might have become even harder.

The logic of network disruptions

Governments intent on using modern communication technologies to their advantage in repressing opposition groups have evidently developed a resourceful set of tools to do so without shutting down all virtual and mobile access for its population. Why, then, do so many countries experience purposefully implemented shutdowns? In theory, there are two types of access denial: the long-term prohibition or restriction of internet access, and shorter, infrequent intermissions of accessibility. As previously discussed, the literature on censorship of the internet indicates that selective content censoring usually happens over longer periods of time, and is principally aimed at repressing collective organization and mobilization of disgruntled citizens (Howard, Agarwal & Hussain, 2011; King, Pan & Roberts, 2013). It is therefore plausible to assume that long-term outages implemented by the government are intended to obstruct (or at least reduce) the mobilization of antigovernment sentiments. Where governments are already threatened by organized groups, such pre-emptive shutdowns are likely to undermine opposition preparations for collective attacks (see also Herreros & Criado, 2009), and should therefore occur *prior* to major battles between the state and its opponents. Whereas sustained outages might be an effective tool to impede the long-term mobilization of opposition groups, they run the risk of motivating dissatisfied people to join protests against this extreme form of censorship.

In contrast to such widespread and enduring content censoring, empirical evidence shows that most incidences of actual 'blackouts' cover a relatively short time span, not least because long-term outages affect a country's reputation and economic capacity (Howard, Agarwal & Hussain, 2011: 220). Since short periods of denied access to the internet are not likely to affect sustained opposition activity, it is plausible to assume that complete shutdowns are implemented in anticipation of temporary advantages over a violently resisting opposition. Short-term shutdowns are therefore likely to be part of a repressive response towards an already mobilized opposition, in order to impede the capability to successfully implement, as well as the ability to coordinate, larger attacks against the state. The following sections discuss in more detail the incentives and costs associated with temporarily shutting down the internet.

Incentives for temporary network outages

The first anticipated benefit of temporarily shutting down network services pertains to opposition groups' capabilities to effectively carry out attacks against the military. Recent conflicts in Libya and Syria provide extensive footage of opposition fighters using online mapping services, such as Google Earth and Google Maps, to accurately locate military targets, and to calibrate weapons to effectively reach said targets (Miller, 2012; Brownstone, 2011; Keating, 2013). Faced with an army that is better equipped with weapons, technology, and trained soldiers, opposition groups frequently conduct asymmetric or 'irregular' warfare (Kalyvas & Balcells, 2010), where reliance on all available means of combat is pivotal. Recent developments of geographical location systems made for personal use on devices such as smart phones and tablets have thus revolutionized their capacity to locate and target regime forces with a level of precision that was not available a decade ago.

Secondly, the ability to coordinate personnel, material, and last-minute strategies via mobile phones and the internet is a vital channel by which opposition groups are able to organize attacks and resistance against the government. The presence of virtual communication channels, accelerated by smart phones, has increased the value of disseminating information and using it as a 'coordinating force [. . .] dramatically' (Shirky, 2008: 159). Additionally, '[b]logging, tweeting, podcasting, and taking pictures and videos and uploading them to Flickr and YouTube can all be done at near-zero financial cost' (MacKinnon, 2012: 24), making these tools available to anyone with a working internet connection. Recent studies report that social networking may in fact lead to increased participation in protest (Tufekci & Wilson, 2012), although these processes are less likely to be permanently affected by short intermissions in access. The internet provides a channel of communication that is fast, cheap, and harder to manipulate than more traditional, centralized media types such as the radio or newspapers (see Edmond, 2011: 25). A recent report interviewing members of the Free Syrian Army (FSA) supports these findings, reporting that:

> [e]very fighter seems to have at least one mobile phone, used to speak with families, Skype [. . .], and even advise Syrian soldiers how to defect to the opposition. Some note the difference a generation can make to the fate of their challenge against the government – and providing video evidence of atrocities and war crimes that are corroding the legitimacy of the regime. (Peterson, 2012)

The threat posed by the increased abilities to coordinate, disseminate information, and even incite military soldiers to join the rebellion is likely to be imminent to authoritarian rulers who fear for their political survival. In response, in a

campaign aimed at repressing and possibly even eliminating the opposition, shutting down these communication channels can constitute a rational policy decision.

Where state-run cell phone and internet services are generally accessible, opposition groups are likely to make use of them. Longer periods without access to state-provided network services should increase the probability of rebel groups finding alternative means and services, such as satellite phones and modems, network access via neighboring countries, or dial-up connections (when landlines are accessible).[5]

The portfolio of surveillance and censorship methods state-run connections can be subjected to is diverse, but when compared to alternatives such as satellite networks, reliance on tools used by the majority of a country's population might still provide more security than using less broadly used channels such as satellite connections. New research in IT security demonstrates how satellite mobile devices produce traceable signals that allow governments to simply locate users and trace messages (see Driessen et al., 2012).[6] When compared to ordinary network connections, locating and targeting rebels who are communicating outside of conventional structures offers a clear coercive advantage for the state.[7] Although opposition groups might therefore possess alternative ways of connecting via cell phone and internet, the increased usage of satellite devices is likely to improve the regime's capability of identifying armed fighters among the civilian population.

The costs of network outages

Shutting down network services not only affects the opposition and its supporters, it affects a country's entire population, not least due to losses in economic revenues. When the Mubarak regime shut down internet services for five days in 2011, the Egyptian economy lost an estimated $90 million worth of revenues (Howard, Agarwal & Hussain, 2011: 231). This figure only includes direct losses in revenues due to the absence of internet and phone services; it does not include the revenues of general communication services, such as those generated by tourism sites, call centers, and e-commerce, as well as potential losses on investment in the aftermath of the blackout (see OECD, 2011).

A population that relies on the internet for both personal and professional reasons is likely to be increasingly skeptical of a government that makes these channels unavailable to them. For example, evidence suggests that in light of the outages Egypt faced in 2011, an increasing number of protesters took to the streets all across the country in order to demonstrate against Mubarak's regime (Hassanpour, 2013). When Turkey's government merely decided to block access to Twitter in April 2014, the response was a national and international rallying of protests against Prime Minister Erdogan (Tufekci, 2014). Obstructing (or even just partly obstructing) accessibility can contrarily provide incentives for a neutral population to participate in antigovernment protest.

Above all, governments pursuing a counter-insurgency strategy in response to political threats are highly dependent on information provided by the civilian population (Lyall, 2010). Cell phone and internet access considerably facilitate communication for civilians willing and able to share crucial information on the location and activities of opposition fighters, without said fighter noticing the correspondence. This 'human intelligence' mechanism (Shapiro & Weidmann, 2015: 5) should ultimately provide the state with an advantage over the rebellion.

Given the incentives and costs for governments in shutting down their networks, cutting all internet access is likely to be most effective in stifling opposition capability when used on an infrequent, temporary basis. However, 'overuse' of this most extreme form of censorship is likely to be counterproductive: if network disruptions precede all forms of military actions and occur on a regular basis, opposition groups will be able to use them as an 'early-warning system'. Following from this, I argue that network outages are likely to be consistently associated with increased fighting. Conversely, not all periods of intense fighting are likely to be accompanied by shutdown networks. In short, disruptions will consistently be part of larger military campaigns, whereas not all military campaigns will entail disruptions.

[5] Opposition groups might decide to reorganize entirely and banish mobile and virtual communication from their coordination repertoire. In such instances, the anticipated benefits from shutting down network services are likely to be low.

[6] Despite research in this field being comparatively new, news reports quoting researchers offer support: 'Radio direction finding and signals intelligence could easily be deployed in this scenario to figure out where the opposition is communicating from,' said John Scott-Railton, a research fellow at the Citizen Lab, an organization at the University of Toronto that focuses on Internet security (Perlroth, 2013). Security researcher Jacob Appelbaum contends: 'Satellite phone systems and satellite networks are unsafe to use if location privacy or privacy for the content of communications is desired. These phone protocols are intentionally insecure and tracking people is sometimes considered a feature' (Jacob Appelbaum, quoted in York & Timm, 2012).

[7] The killings of two journalists in Homs in February 2012 support the notion that governments are making use of this technology. Security specialists contend that the Syrian government is likely to have directly targeted the houses from which they had traced the phones' signals (York & Timm, 2012).

Coercive response or cover-up?

Contemporary conflicts are being documented and simultaneously shared with the outside world through the help of the internet (Diamond, 2010). An alternative explanation for outages in contentious situations could be the government's intention of covering up and hiding violent acts from international scrutiny. Where a regime already receives increased international attention for repressing its citizens, cutting network activities might be part of an attempt to limit the extent of information leaving the country. Disruptions could present a chance to commit more large-scale acts of violence against the population, attempting to 'drain [. . .] the sea' (Valentino, Huth & Balch-Lindsay, 2004: 385) and eliminating the opposition, without creating a national and international audience, thereby potentially increasing the risk of sanctions, interventions, or even a referral to the International Criminal Court. Although autocratic regimes frequently engage in large-scale violence even when the international community is watching, the less real-time information is available, the more likely leaders will be able to plausibly deny responsibility for these atrocities (Mitchell, 2004).[8] The unprecedented number of journalists being killed in Syria demonstrates that the regime is evidently not indifferent about the coverage of the conflict. According to the Committee to Protect Journalists (CPJ), Syria was the most dangerous country to be working in as a journalist in 2012 and 2013, with at least 61 killed between 2011 and 2013; CPJ further reports at least 60 kidnappings of press staff in 2013, as well as journalists being tortured to death (Beiser, 2013).

The cover-up argument has been voiced by international advocacy groups, such as Amnesty International, which has stated that:

> [a]s fighting intensifies [. . .] we are extremely worried that the news that internet and mobile phone services appear to have been cut throughout Syria may herald the intention of the Syrian authorities to shield the truth of what is happening in the country from the outside world.[9]

The intended effect of a disruption should therefore be an 'unobserved' increase in government repression. Although more atrocities are occurring, the groups collecting and disseminating the details on these events might have reduced access to their informants who usually provide evidence on individual victims.

The victims of violence during outages

Whether the victims of government violence change during internet outages likely depends on the government's motivation for the shut-down. Following international law, the literature on state repression broadly differentiates between combatant and non-combatant victims, while acknowledging that this distinction is often intentionally or unintentionally ignored by governments (Downes, 2011). Threatened governments are likely to intentionally conflate the status of combatants and civilians in irregular civil conflicts, where the organization of the opposition is opaque and front lines between groups are unclear (Valentino, Huth & Balch-Lindsay, 2004; Balcells, 2010). As such, the Syrian regime has conducted the type of atrocious campaign against both rebel fighters and non-combatants that assumes that anyone not showing explicit support is opposed to the regime.

If the intent behind shutting down the internet is to cover up prosecutable war crimes against unarmed civilians, it is plausible to assume that the composition of victims of government violence changes during outages, since the explicit focus of these disruptions would then be to attack as many civilians as possible. Empirically, a significant increase of – possibly unobserved – violence that only occurs *during* outages should therefore indicate a higher proportion of civilians killed.

With recent research indicating that censoring or blocking of the internet can lead to an increased turnout of protesters taking to the streets, an alternative reason for a higher proportion of civilian casualties would be if governments decided to then violently crack down on these protesters. Empirically, a substantial increase in violence in the *immediate aftermath* of outages would offer support for this scenario.

In this article, I argue that governments selectively implement outages as part of particularly repressive responses to increased armed opposition resistance. Where shutdowns are part of a concerted repressive response, the most substantial increase in violence should begin prior to, and then continue throughout, outages. In the midst of fighting, it is plausible to assume that anyone deemed to belong to the opposition – including armed fighters and civilians standing by – is likely to be indiscriminately attacked.

Testable implications

If governments use network disruptions as a military tactic that forms part of a concerted repressive offensive

[8] For coverage on the Syrian regime's plausible deniability of other events, such as the chemical attack in Ghouta in 2013, see Beaumont (2013).

[9] Ann Harrison, Middle East and North Africa Programme, Deputy Director Amnesty USA (Amnesty International, 2012).

Table I. Expected effects for network disruptions and violence

Expectation	*Documented*	*% undocumented*	*Timing of increase*
Coercive response	Increase	No change	**Prior**/during disruption
Cover-up	No change/increase	Increase	**Only during** disruption
No effect	No change	No change	

against opposition groups, a main observable outcome is an increase in the activity of pro-government fighters during and in the immediate time surrounding outages. Pro-government fighter activity is measured by the number of people killed by the regime. According to the theoretical expectations laid out above, I expect short, unexpected network outages to be accompanied by significantly higher levels of military activity, and thus significantly higher numbers of people killed. The *actual* number of people killed is defined as the combined number of *documented* and *undocumented* fatalities.[10] In order to understand whether disruptions are linked to higher levels of violence, it is crucial to account for changes in documented and undocumented violence, since changes in communication technology might have an effect on the documentation process. The main empirical expectation, given that disruptions are part of a state's set of military tactics, is:

> *Hypothesis 1:* All else equal, periods of network disruption are accompanied by a significant increase in actual conflict fatalities.

The main alternative explanation is that governments use disruptions to cover-up their atrocities:

> *Alternative hypothesis:* All else equal, the proportion of undocumented conflict fatalities increases significantly during network disruptions.

Whereas the number of undocumented cases is seldom zero, the alternative explanation for why governments cut their networks is that they do this to cover up their crimes, which means the dark figure of unreported cases should increase disproportionately to the number of documented cases. A further possible scenario is that governments intend to cover their tracks, but that they are unsuccessful at doing so. An additional factor is therefore considered, which is the timing of violence versus network disruptions. If governments care about the news of atrocities travelling beyond the battle grounds, they are likely to only *commence* the violence once the network is disconnected. Starting a campaign of violence and then shutting out the international community is likely to raise more awareness than before. In short, cover-up campaigns should show no signs of an increase of violence *prior to* the outage, and if successful, should hide a large increase in undocumented fatalities *during* the disruption. In contrast, increases in violence immediately preceding disruptions are consistent with the coercive response hypothesis. I expect increases in military activity *prior to* and *during* disruptions to indicate the strategic value of shutdowns in government repression policy.

Table I summarizes the expectation of the main hypotheses and the alternative explanation for documented violence, the percentage of undocumented violence, and the timing of violence prior to and on days with network disruptions.

Empirical strategy

Network outages in the Syrian civil war

Syria's government has a demonstrated history of blocking content on the internet (OpenNet Initiative, 2009; Deibert, 2008). Since the start of the civil conflict, there have been two main types of internet disruptions: national, large-scale outages and smaller regional variations in accessibility. This article only analyzes large-scale national incidences of complete network outages. There is strong evidence that confirms the large-scale outages to have been directly implemented by the Syrian government (Gallagher, 2012). Furthermore, news reports confirm that country-wide network outages are simultaneously accompanied by the disruption of cell phone services.[11] These outages have occurred at irregular intervals, without being anticipated by either the international media or the opposition groups.

[10] Actual levels of violence, meaning documented and undocumented cases combined, are not directly observable. As will be discussed in more detail below, the availability of five different sources for the Syrian case allows me to estimate the number of undocumented cases.

[11] See, for example, http://www.bbc.co.uk/news/technology-20546302.

Local intermissions generally occur in parts of the country that are already controlled by opposition groups, most notably the northern governorates Ar-Raqqah and Al-Hasaka. These two governorates have experienced limits in accessibility to the internet for most of the period under investigation. Syrian security experts contend that these deteriorated connections occur in regions where the opposition has taken control of territories, in an effort to withhold public goods from a population that is 'collaborating' with the regime's enemies.[12]

The country-wide outages for the period between March 2011 and September 2013 are determined through the information collected by the Google Transparency reports on traffic disruptions in Syria since March 2011.[13] Suspensions of traffic that lasted between a few hours and three days occurred in June 2011, July 2012, November 2012, January 2013, and twice in May 2013.[14] To account for the empirical expectations of the theory, I include three different treatments for network outages. The first dichotomous variable takes on the value of 1 on days where the traffic was disrupted, and 0 for days of normal connection. The second variables sets the treatment at t–1, the day prior to the disruption. The third variable looks at the time window of the disruption, and codes the day prior to, the days of the disruption, and the following day as 1, and the rest as 0. To control for decreasing or increasing effects over time, I include a measure that accounts for the number of previous outages, as well as a variable that measures the time since the last outage, as recent outages might positively or negatively affect the dynamics of violence.

Documented conflict fatalities

I make use of data that combine information on fatalities in Syria that were collected by five organizations that have been continuously working since the outset of the conflict. In order to assure the highest possible quality standards in combining documented evidence from different sources, records of fatalities are only included if they are identifiable by full name of the victim, date of death, and governorate in which the death occurred. The records are available at a daily level for each of the country's 14 governorates; further geographical disaggregation is not possible. The five sources included in the analysis are the Syrian Center for Statistics and Research (SCSR),[15] the Syrian Network for Human Rights (SNHR),[16] the Syrian Observatory for Human Rights (SOHR),[17] the Syria Shuhada (SS) Website,[18] and the Violations Documentation Centre (VDC).[19]

To create a complete and accurate list of documented killings these data need to be processed in two different ways: first, duplicates within individual lists have to be identified and removed. Fatality recording is conducted in the midst of chaos and fighting, making it highly probable that the same victim is recorded more than once by the same organization. This inflation of counts is likely to be non-random, as more visible attacks might lead an increased number of survivors to report the same victims. Second, victim identities need to be linked across lists, in order to arrive at an overall number of documented victims. These procedures were initially done for the period from March 2011 to April 2013, and a second round was conducted for the period from May to September 2013 (both conducted by Price et al., 2013, 2014). For the second period, the dataset only includes linked fatalities from four sources.[20] For the period from March 2011 to April 2013, Price et al. (2013) included 256,455 records from the five sources mentioned above in the record-linkage process, and arrive at a total number of 90,769 victims documented by these five sources.

The data used in this analysis include both combatant (such as belonging to the Free Syrian Army) and non-combatant victims killed by the Syrian government and pro-government forces. The data do not allow for an exact classification of victims into these two categories; instead they are classified as 'martyr' deaths by the recording groups, indicating that state military, paramilitary, and other higher ranking government officials are excluded. Since the theoretical expectations formulated in this article pertain to an increase in both combatant and non-combatant fatalities, these compiled data present an appropriate measure for government repression.

[12] Personal communication with Dlshad Othman (Kurdish Syrian Activist and Internet Freedom Fellow), Anas Qtish (Syrian Blogger, Electronic Frontier Foundation), and staff of the Syrian Digital Security Monitor.

[13] See http://www.google.com/transparencyreport/traffic/.

[14] The fraction of normalized worldwide traffic in Syria is presented for a sample of outages in the online appendix.

[15] http://csr-sy.org/

[16] http://www.syrianhr.org/

[17] http://syriahr.com/

[18] http://syrianshuhada.com/

[19] http://www.vdc-sy.org/

[20] See Price et al., 2013: Appendix C. Records from the Syrian Observatory for Human Rights were not made available after April 2013. However, analysis of the matched data prior to May 2013 reveals that the contribution of records that are only identified by one source is approximately 5%, making matched data with four sources comparable to matching with five sources.

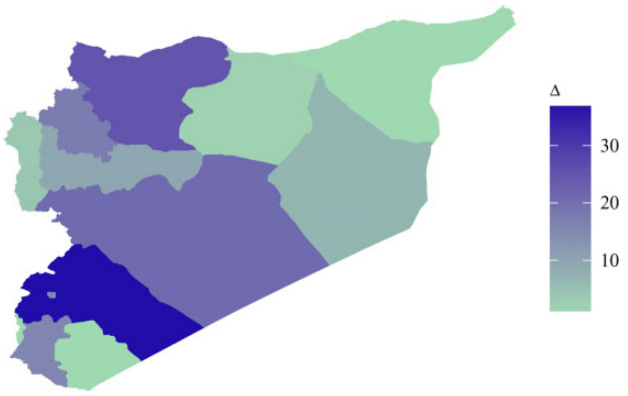


Figure 1. Mean difference in daily killings between days with and without internet

Network outages and documented killings

Descriptive evidence. The descriptive difference of documented daily killings during network outages is presented in Figure 1, which maps the average difference in daily killings between days where the internet is turned on and days where the country is disconnected. In the north-east of the country, opposition groups have established quasi-administrative structures (MacFarquhar & Saad, 2012) and consequently have been cut off from central government services, including the internet, which means that national outages are likely to display little effect in these regions. Evidently the effect depends on the degree of armed confrontation between opposition and government groups, which means that subnational variations need to be taken into account in the analysis. The north-west of the country, where Aleppo and Idlib are located, show more than 20 additional fatalities on days where there is no internet across the country, compared to other days during the period under investigation. The conflict centers of Rural Damascus and Homs in the center of the country show an average increase of more then 30 fatalities.

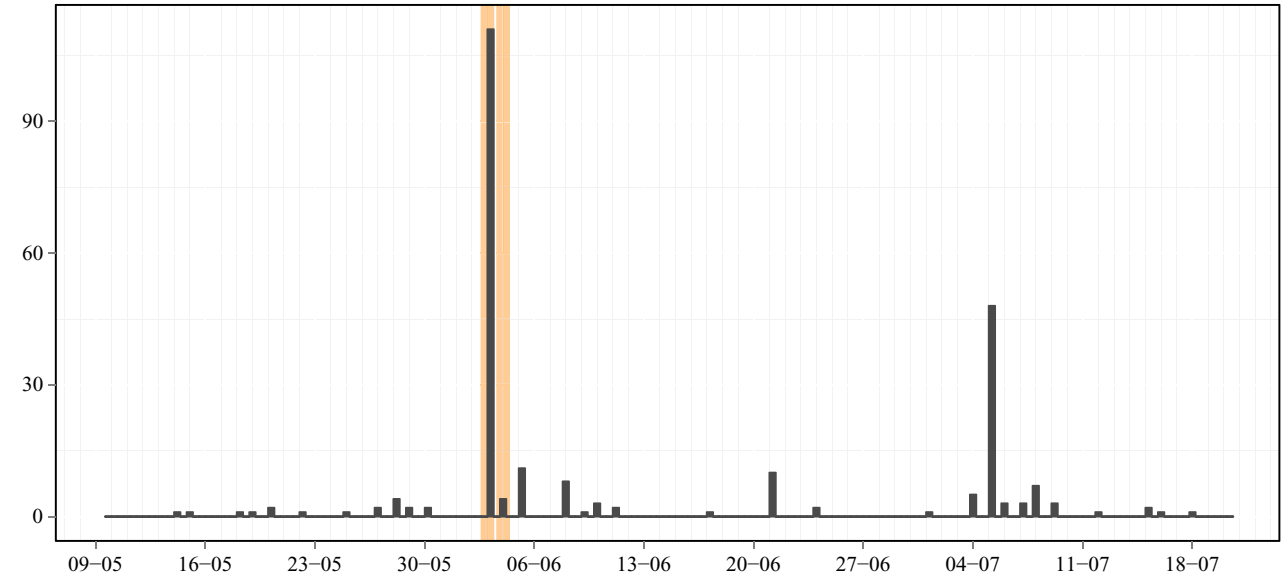
To further investigate the relationship between violence and disruption it is useful to visually inspect the dynamics of violence and disruptions across time. Figure 2(a) plots the daily counts for Hama from May to August 2011; the shaded area marks the disruption days in June. A sharp increase in violence on the first day of the outage is clearly visible in this graph. A different trend is shown in Figure 2(b), which plots the daily counts for Rural Damascus across May to August 2012. As can be seen quite clearly, the number of killings rises substantially on the day *before* the blackout, decreases on the day concerned to a nevertheless high number, and increases slightly on the following day. This visual inspection indicates that the association between disruptions and increases in violence moves beyond the mere outage days. As discussed above, network disruptions implemented as part of a coercive response need not necessarily be implemented prior to the commencement of fighting. Shutting down the network amidst fighting is likely to constitute a role in a military strategy.

National-level evidence. Since the outages occur at a national level, the first step of the multivariate analysis examines the national effect with daily data from 15 March 2011 until 30 September 2013. Since the conflict in Syria has intensified over time, the event count of killings follows a generally increasing, non-mean-reverting trend. To account for these dynamics, I estimate a Poisson exponentially weighted moving average model (PEWMA), as formalized by Brandt et al. (2000). The PEWMA is a structural time-series model that nests a Poisson model, where observed counts at time t are modeled as a weighted average of counts at previous time points (Brandt et al., 2000: 827).[21] Since the interpretation of the coefficients is not straightforward, I calculate the predicted percentage changes in violence for the same three treatments used in the difference of mean tests. Table II reports the results of the three models. The model predicts that on average, the level of violence increases by 26.3% on the day prior to an internet outage. During the actual blackout, violence is predicted to increase by 8.6%, and when looking at the time window, the average increase is predicted to be almost 47%. Although not all governorates are affected by fighting in the same way, the aggregate national evidence offers further support for the hypothesis that outages are preceded and accompanied by significant increases in violence.

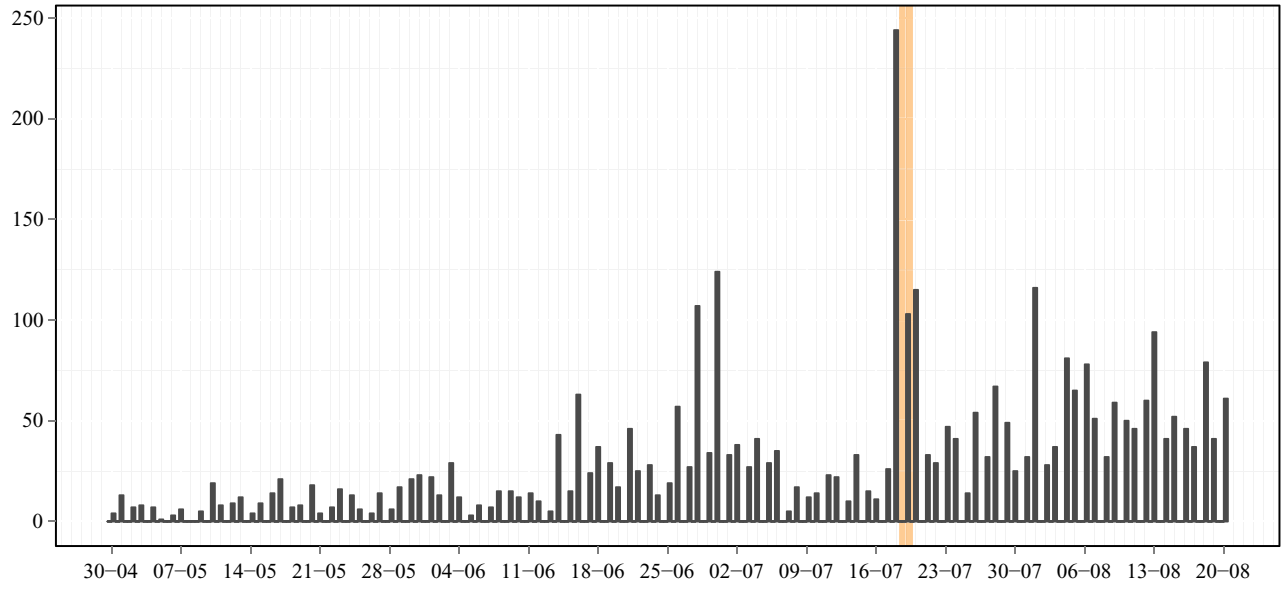
Regional evidence. Since the level of fighting varies substantially across the different regions in Syria, I estimate a time-series cross-section fixed-effects Poisson model, where the 14 governorates are the fixed units.[22] I simulate the expected change in the number of regime fatalities in each Syrian governorate between a day where all networks are available versus a day where they are shut down. Figure 3 shows all 14 governorates along the x-axis and plots the expected change in fatalities including the 95% confidence interval on the y-axis. The lower (yellow)

[21] The model estimates a hyperparameter ω that accounts for dependence of the event counts over time, where values close to 0 indicate more dependence, and values approaching 1 indicate few dynamics, and a data structure that could potentially be modeled with a conventional Poisson model. I thank Patrick Brandt for providing the estimation code on his website: https://www.utdallas.edu/~pbrandt/pests/pests.htm.

[22] See Table AII in the online appendix for the regression table. I include lagged dependent variables at t–1 and t–2 to control for previous levels of violence.



(a) Hama 2011



(b) Rural Damascus 2012

Figure 2. Violence and network disruptions

lines show the expected change on the day of network outages, and the upper (blue) lines show the expected effect on the day prior to an outage. None of the confidence intervals include zero, which means that the days with network disruptions witness statistically significant higher levels of violence across all Syrian governorates. In both models, the substantive effect varies clearly across governorates, which is not surprising given the significant differences in the levels of violence experienced. In Homs and Rural Damascus, days without internet (yellow lines) experience at least three additional incidences of lethal violence when compared to days with regular access. The effect of network outages on violence seem less pronounced in peripheral regions such as As-Suwayda, Al-Hasaka, and Quneitra.

On days prior to internet disruptions, the estimated expected changes in violence are substantially larger. The expected increase in conflict fatalities in Homs, Rural Damascus, Aleppo, and Idlib is above ten. Both models offer support for the coercive response argument: governorates in Syria experience a significant increase in conflict

Table II. National-level time-series model: Disruptions and violence

	1	*2*	*3*
Pre disruption	0.233 (0.105)		
	26.3%		
Disruption		0.083 (0.098)	
		8.6%	
Time window			0.383 (0.087)
			46.7%
Last disruption	0.001 (0.000)	0.001 (0.000)	0.001 (0.000)
ω	0.063 (0.002)	0.063 (0.002)	0.064 (0.002)
N	851	851	851
LLF	–4,581.051	–4,582.848	–4,573.671
AIC	9,166.101	9,169.696	9,151.343

Poisson exponentially moving average (PEWMA) model. Standard errors in parentheses. Predicted precentage changes in bold.

deaths perpetrated by the regime on days where the regime shuts down network services. Furthermore, a first substantial increase in violence occurs one day prior, an increase we would not expect if the regime were interested in covering up atrocities during blackouts or cracking down on a higher number of protesters as a result of the outages.

Robustness

Due to the dynamic nature of conflict violence, it is important to test whether the results are being driven by general conflict trends in the data. I additionally test whether the results hold when replacing absolute levels of documented violence with the first difference, where the dependent variable only reports the change in fatalities between two days. The first model in Table III tests for an increase in violence on the days prior to disruptions, the second model tests for the first day of actual disruptions, and the last model tests for the day afterwards, in order to investigate whether violence continues to rise. As expected, the most statistically significant and substantive increase is found on the day prior to the disruption. The effect on the actual days with outages is not as pronounced, and there seems to be no enduring effect once networks are turned back on again.

Given the small number of 'treatment' incidences over the time period of three years it is important to check whether these results might be due to chance.[23] A useful way to do this is to use a placebo test (see Dafoe & Tunón, 2014).[24] In order to maintain the structure of the treatment variable, I create a series of time-shifted placebos (see Reynolds, 2014; Dube, Kaplan & Naidu, 2011), where the treatment is moved between t–30 and t+30 intervals, to account for the time period one month prior to and one month following each outage.[25] For each placebo, the national-level time-series count model is estimated, and the predicted percentage change of violence on days with the treatment saved. Figure 4 plots the predicted changes, as well as the actual treatments at t (the disruption) and t–1 (the day prior to the disruption). The majority of all placebos predict a change in violence that is negative, or less than +2%. Importantly, the predicted changes in the immediate aftermath of outages are either zero or negative, further confirming that governments are not responding to an increase in protest during the disruption.

Documentation patterns of violence during outages

The conflict in the Syrian Arab Republic presents one of the most sophisticated real-time documentation efforts in the history of casualty recording with countless groups and organizations working to record violence. As in all conflicts, however, it is impossible to determine the true population of conflict fatalities via documented data. Human rights groups are doing their very best to document all violence that is documentable, but for analyses such as the one attempted in this article, it is of paramount importance to obtain an estimate of *all* fatalities, not just those documented. Studies examining the effect of information technology on the intensity of violence are particularly sensitive to potential biases in conflict data that might arise precisely because of changes in said technology. This study is no different, and the cover-up hypothesis even supports this claim.

One way to test for the cover-up hypothesis is to determine whether the level of underreporting differed substantially on days without internet compared to days with network access. Since four datasets are deduplicated and matched for the entire observation period, the overlap structures of fatalities that were recorded by one, two, three or four sources can be used to estimate the number of fatalities that were not documented by any source (Gohdes, 2014). Log-linear capture-recapture estimation follows this simple intuition and has been used to estimate fatalities in a multitude of conflicts (see Lum, Price & Banks, 2013).[26] I

[23] Recent revelations by US National Security Agency (NSA) whistleblower Edward Snowden suggest that the November 2012 outage might have occurred due to a technical failure brought about by the NSA (Bamford, 2014).

[24] I thank an anonymous reviewer for suggesting this.

[25] The placebos created were at t [–30,–25,–20,–15,–10,–5,+1,+5,+10,+15,+20,+25,+30].

[26] Log-linear Poisson models for capture-recapture estimation are implemented in the R package Rcapture (Baillargeon & Rivest, 2007). Log-linear models are effective at dealing with capture heterogeneity and list dependencies, two of the main challenges when estimating conflict fatalities (see Manrique-Vallier, Price & Gohdes, 2013).

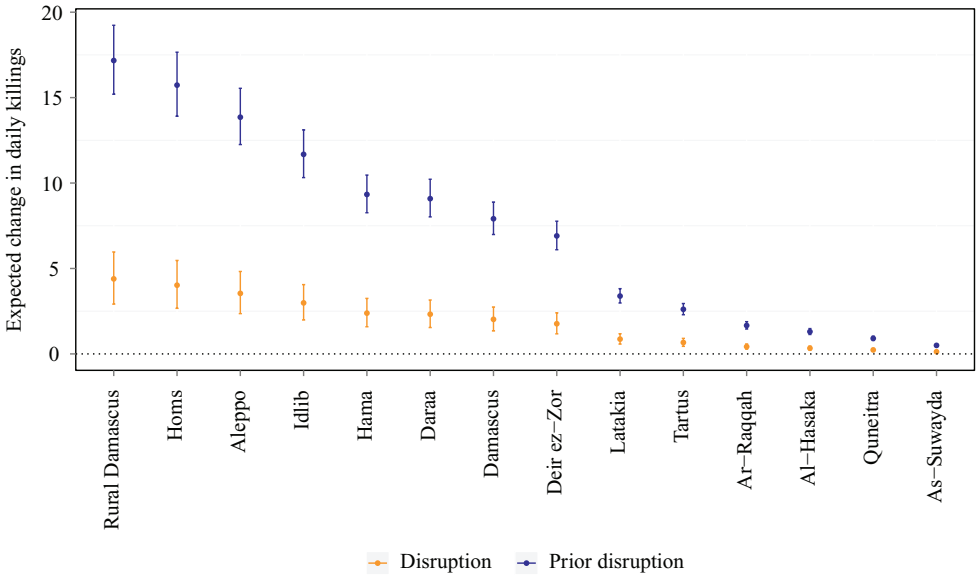


Figure 3. Expected change in daily killings, given network disruptions

Table III. First difference model: Network disruptions and changes in violence

	4	*5*	*6*
(Intercept)	–0.270	–0.251	–0.256
	(0.187)	(0.187)	(0.188)
Pre disruption	5.743		
	(1.596)		
First day		3.539	
		(3.323)	
Post disruption			1.044
			(1.466)
Last disruption	0.002	0.002	0.002
	(0.001)	(0.001)	(0.001)
No. disruptions	0.384	–0.437	0.381
	(0.376)	(0.852)	(0.376)
Diff_{t-1}	–0.599	–0.600	–0.600
	(0.009)	(0.009)	(0.009)
Diff_{t-2}	–0.273	–0.273	–0.273
	(0.009)	(0.009)	(0.009)
R^2	0.281	0.280	0.280
Adj. R^2	0.280	0.280	0.280
N	11,914	11,914	11,914

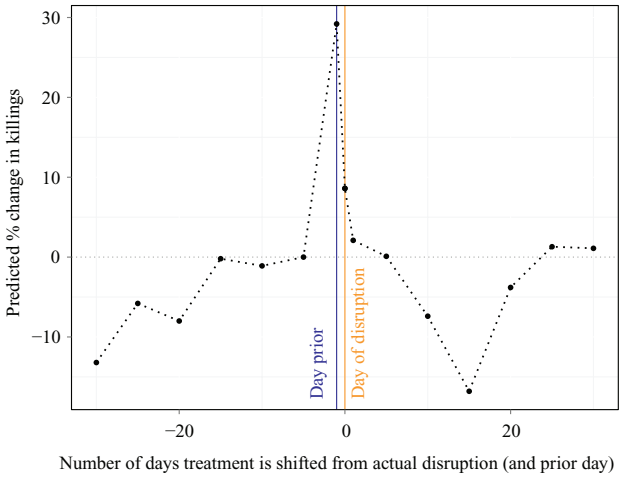


Figure 4. Time shifted placebo treatment test

isolate the number of documented fatalities by governorate for the days without internet, and estimate the number of undocumented killings for each of these periods and regions separately. Since the degree of underreporting is likely to vary across time and space, I select the fixed period of a week prior to each network disruption and estimate the level of underreporting at the national level, and for each respective governorate as well. I then compare the levels of regional underreporting of the immediate time period prior to the disruption with the underreporting during the disruption in order to assess whether or not disconnected days lead to systematic underreporting of violence.

For example, during the internet blackout on 3 and 4 June 2011, 24 victims were documented in Aleppo. Only seven of these victims are reported in all lists; the remaining victims were reported by a combination of less than all sources. Capture-recapture estimation reveals that it is highly likely that 42 individuals were killed in this period (with a 95% confidence interval of [25, 150]), which means that 42.7% of all victims went undocumented in those two days. In the week prior to the June outage, 133 victims of regime violence were documented in

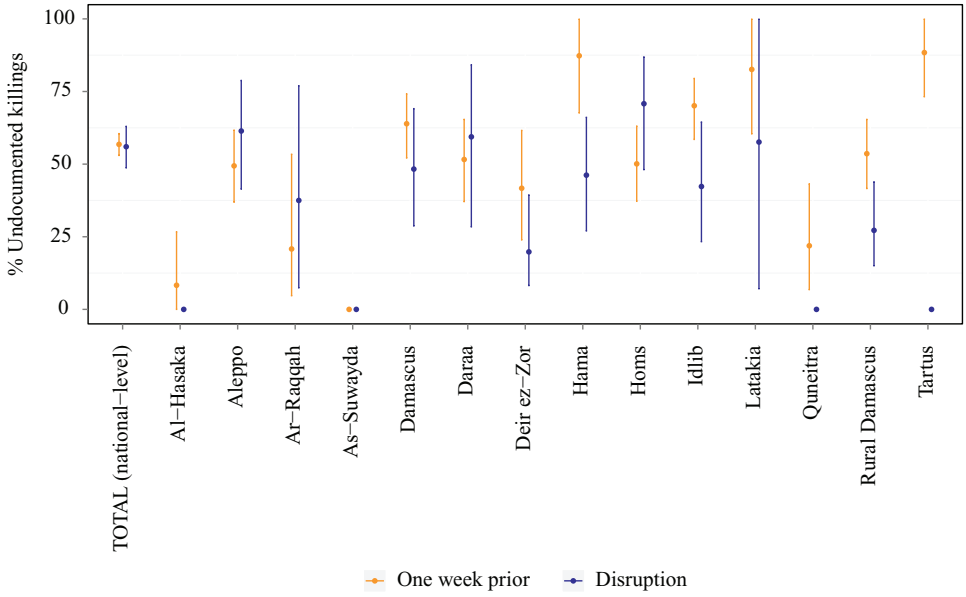


Figure 5. Percentage of undocumented fatalities one week prior to and during disruptions

Aleppo, of which only 46 were known by all sources. The estimated number of actual regime fatalities is 167 [c.i.: 146, 212], which means that 20.4% of all cases went undocumented.

Figure 5 shows the level of underreporting for the week prior to, and during internet outages at the national and governorate level, including 95% confidence intervals. At the national level, the degree of underreporting is almost exactly the same, and at the governorate level, only Hama displays a significant difference, but in this case underreporting was significantly higher *prior to* the outage, which poses no problem for the validity of the results. The results suggest that documentation patterns are not systematically linked to network outages. Whereas variation in reporting across governorates is partly visible, it is likely to be driven by other factors not addressed in this study.

Conclusion

Censorship of the internet is nothing new: authoritarian regimes intent on maintaining the status quo within their country have been relatively successful at manipulating content in their favor (Morozov, 2012; Rød & Weidmann, 2013). What has remained unclear to date, however, is to what extent extreme forms of censorship – such as the cutting of all connections – have the potential for constituting a tactic within larger military offensives. The results of the analysis of network outages and daily conflict fatalities in Syria suggest that regimes implement large-scale disruptions selectively and purposely in conjunction with launching larger battles. Evidently, not all battles are accompanied by outages, but when they are, they tend to be preceded by a substantial increase in violence.

Even in conflicts that are under as much national and international scrutiny as the current case of Syria, it is important to analytically distinguish between the empirical implications for *documented* violence and the empirical implications for *actual* levels of violence: cases that are observed and those that are either intentionally or unintentionally hidden from documentation. The theoretical expectations advanced in this article clearly distinguish between implications for violent documentation and violence in general. Distinguishing between the documented and the dark figure of violence improves the analytical leverage of the article's findings: the fact that undocumented violence in Syria is not systematically affected by short disruptions offers important support for the coercive response hypothesis.[27] Estimating the degree of underreporting, however, also demonstrates the variability in documentation. Cases where more violence is hidden from view during disruptions might turn out to be a welcome side-effect for governments seeking to maintain international legitimacy and internal control.

[27] Incidences where the shutdown lasts much longer might produce very different results.

This article has attempted to understand why governments might have an incentive to include the disruption of internet and cell phone service in their military strategy. I have argued that the scarce and sudden disconnection from essential communication networks is likely to weaken opposition groups' propensity to organize, but further research is needed in order to understand whether this is in fact the case, and if so, what the exact underlying mechanisms are that allow network failures to get in the way of effective information dissemination. This analysis has investigated the effects of nationwide outages, and additional research is needed to understand the logic of regional variations in network accessibility.

Syria presents the first conflict that has been meticulously followed and fuelled by a vast online audience: by the opposition fighters and supporters, by regime forces and their supporters, and by the outside world at large. The increasing importance of establishing control over content on and access to the internet is likely to exercise a growing appeal on regimes eager to adjust their repertoire of repressive tools in dealing with new digital threats to their stability.

Replication data

The dataset and replication files for the empirical analysis in this article, along with the online appendix, can be found at http://www.prio.no/jpr/datasets.

Acknowledgements

A previous version of this article was presented at the ISA Annual Conference 2014. I thank Michael Colaresi, Bethany Lacina, Kathleen Gallagher Cunningham, Jessica Maves Braithwaite, David Siegel, Will Moore, Cullen Hendrix, Sabine Carey, Nikolay Marinov, Evangeline Reynolds, Nils Weidmann, and the participants of the Workshop on 'Communication, Technology and Political Conflict' at Yale University for helpful comments.

References

Aday, Sean; Henry Farrell & Marc Lynch (2010) Blogs and bullets: New media in contentious politics. United States Institute of Peace Peaceworks 65 (http://www.usip.org/publications/blogs-and-bullets-new-media-in-contentious-politics).

Amnesty International (2012) Syria: Shutting down of internet and mobile networks alarming development. Press release, 29 November (http://www.amnesty.org/en/for-media/pressreleases/syria-shutting-down-internet-and-mobile-networks-alarming-development-2012-).

Baillargeon, Sophie & Louis-Paul Rivest (2007) Rcapture: Loglinear models for capture-recapture in R. *Journal of Statistical Software* 19(5): 1–31.

Balcells, Laia (2010) Rivalry and revenge: Violence against civilians in conventional civil wars. *International Studies Quarterly* 54(2): 291–313.

Bamford, James (2014) Edward Snowden: The untold story. *WIRED*, August.

Beaumont, Peter (2013) Syrian missiles similar to 'ones used in previous chemical weapons attacks'. *Guardian* 22 August (http://www.theguardian.com/world/2013/aug/22/syria-missiles-similar-chemical-weapons-attack).

Beiser, Elana (2013) Syria, Iraq, Egypt most deadly nations for journalists. Committee to Protect Journalists Special Report 30 December (http://cpj.org/reports/2013/12/syria-iraq-egypt-most-deadly-nations-for-journalis.php).

Brandt, Patrick T; John T Williams, Benjamin O Fordham & Brian Pollins (2000) Dynamic modeling for persistent event-count time series. *American Journal of Political Science* 44(4): 823–843.

Breuer, Anita; Todd Landman & Dorothea Farquhar (forthcoming) Social media and protest mobilization: Evidence from the Tunisian revolution. *Democratization*. DOI: 10.1080/13510347.2014.885505.

Brownstone, Andy (2011) Meet the Libyan rebels on the front line. BBC Newsbeat 24 May (http://www.bbc.co.uk/newsbeat/13505340).

Dafoe, Allan & Guadalupe Tunón (2014) Placebo tests for causal inference. Paper presented to the annual meeting of the International Studies Association, Toronto.

Deibert, Ronald (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, Ronald & Rafal Rohozinski (2010) Control and subversion in Russian cyberspace. In: Ronald Deibert (ed.) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 15–34.

Diamond, Larry (2010) Liberation technology. *Journal of Democracy* 21(3): 69–83.

Downes, Alexander B (2011) *Targeting Civilians in War*. Ithaca, NY: Cornell University Press.

Driessen, Benedikt; Ralf Hund, Carsten Willems, Christof Paar & Thorsten Holz (2012) Don't trust satellite phones: A security analysis of two satphone standards. *IEEE Symposium on Security and Privacy*: 128–142.

Dube, Arindrajit; Ethan Kaplan & Suresh Naidu (2011) Coups, corporations, and classified information. *Quarterly Journal of Economics* 126(3): 1375–1409.

Edmond, Chris (2011) Information manipulation, coordination, and regime change. NBER Working Paper no. 17395 (http://www.nber.org/papers/w17395).

Gallagher, Sean (2012) Updated: Paint it black – how Syria methodically erased itself from the 'net. *Ars Technica* 1 December (http://arstechnica.com/information-technology/2012/12/paint-it-black-how-syria-methodically-erased-itself-from-the-net/).

Gohdes, Anita R (2014) Predicting unreported conflict fatal ities with log-linear multiple recapture models. Paper presented at Visions in Methodology conference, Hamilton.

Hassanpour, Navid (2013) Media disruption and revolutionary unrest: Evidence from Mubarak's quasi-experiment. *Political Communication* 31(1): 1–24.

Herreros, Francisco & Henar Criado (2009) Pre-emptive or arbitrary. *Journal of Conflict Resolution* 53(3): 419–445.

Howard, Philip N & Muzammil M Hussain (2011) The role of digital media. *Journal of Democracy* 22(3): 35–48.

Howard, Philip N; Sheetal D Agarwal & Muzammil M Hussain (2011) When do states disconnect their digital networks? Regime responses to the political uses of social media. *Communication Review* 14(3): 216–232.

Kalyvas, Stathis & Laia Balcells (2010) International system and technologies of rebellion: How the end of the Cold War shaped internal conflict. *American Political Science Review* 104(3): 415–429.

Keating, Joshua (2013) Firing mortars? There's an app for that. *Slate* 18 September.

King, Gary; Jennifer Pan & Margaret E Roberts (2013) How censorship in China allows government criticism but silences collective expression. *American Political Science Review* 107(2): 326–343.

Lum, Kristian; Megan E Price & David Banks (2013) Applications of multiple systems estimation in human rights research. *American Statistician* 67(4): 191–200.

Lyall, Jason (2010) Are coethnics more effective counterinsurgents? Evidence from the second Chechen war. *American Political Science Review* 104(1): 1–20.

Lynch, Marc; Deen Freelon & Sean Aday (2014) Blogs and bullets III: Syria's social mediated war. United States Institute of Peace Peaceworks 91 (http://www.usip.org/publications/syria-s-socially-mediated-civil-war).

MacFarquhar, Neil & Hwaida Saad (2012) Rebel groups in Syria make framework for military. *New York Times* 7 December.

MacKinnon, Rebecca (2012) *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Madory, Doug (2013) Internet blackout in Sudan. *Renesys Blog* 25 September (http://www.renesys.com/2013/09/internet-blackout-sudan/).

Manrique-Vallier, Daniel; Megan E Price & Anita R Gohdes (2013) Multiple systems estimation techniques for estimating casualties in armed conflict. In: *Counting Civilian Casualties: An Introduction to Recording and Estimating Nonmilitary Deaths in Conflict*. New York: Oxford University Press, 165–182.

Miller, Elhanan (2012) Syrian opposition uses home-made rockets and Google technology, video reveals. *Times of Israel*, 20 August (http://www.timesofisrael.com/syrian-opposition-uses-home-made-rockets-google-technology-new-video-reveals/).

Mitchell, Neil J (2004) *Agents of Atrocity: Leaders, Followers, and the Violation of Human Rights in Civil War*. New York: Palgrave Macmillan.

Morozov, Evgeny (2012) *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

OECD (2011) The economic impact of shutting down internet and mobile phone services in Egypt. 4 February (http://www.Oecd.org/countries/Egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm).

OpenNet Initiative (2009) Internet filtering in Syria (https://opennet.net/sites/opennet.net/files/ONI_Syria_2009.pdf).

Perlroth, Nicole (2013) Syria loses access to the internet. *New York Times Bits Blog* 7 May (http://bits.blogs.nytimes.com/2013/05/07/syria-loses-access-to-the-internet/).

Peterson, Scott (2012) Syria's iPhone insurgency makes for smarter rebellion. *Christian Science Monitor* 1 August (http://www.csmonitor.com/World/Middle-East/2012/0801/Syria-s-iPhone-insurgency-makes-for-smarter-rebellion).

Pierskalla, Jan H & Florian M Hollenbach (2013) Technology and collective action: The effect of cell phone coverage on political violence in Africa. *American Political Science Review* 107(2): 207–224.

Price, Megan E; Jeff Klingner, Anas Qtiesh & Patrick Ball (2013) Updated statistical analysis of documentation of killings in the Syrian Arab Republic. Report commissioned by the Office of the UN High Commissioner for Human Rights (http://www.ohchr.org/Documents/Countries/SY/HRDAG-Updated-SY-report.pdf).

Price, Megan E; Jeff Klingner, Anas Qtiesh & Patrick Ball (2014) Data on killings in the Syrian Arab Republic: May–September 2013. Unpublished dataset. San Francisco: Human Rights Data Analysis Group, January.

Reynolds, Evangeline M (2014) Best of all plausible worlds? Checking robustness of time-series cross-sectional models with fictitious plausible alternate treatments. Paper presented at Visions in Methodology conference, Hamilton.

Rød, Espen Geelmuyden & Nils B Weidmann (2015) Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research* 52(3): 338–351.

Shapiro, Jacob N & Nils B Weidmann (2015) Is the phone mightier than the sword? Cell phones and insurgent violence in Iraq. *International Organization* 69(2): forthcoming.

Shirky, Clay (2008) *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin.

Tufekci, Zeynep (2014) The day the Turkish government banned itself from Twitter. *Medium: Technology and Society* 2 April (https://medium.com/technology-and-society/the-day-the-turkish-government-banned-itself-from-twitter-778b806e38e3).

Tufekci, Zeynep & Christopher Wilson (2012) Social media and the decision to participate in political protest: Observations from Tahrir square. *Journal of Communication* 62(2): 363–379.

Valentino, Benjamin A; Paul Huth & Dylan Balch-Lindsay (2004) Draining the sea: Mass killing and guerrilla warfare. *International Organization* 58(2): 375–407.

York, Jillian & Trevor Timm (2012) Satphones, Syria, and surveillance. *EFF Deeplinks Blog* 23 February (https://www.eff.org/deeplinks/2012/02/satphones-syria-and-surveillance).

Youmans, William L & Jillian C York (2012) Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of Communication* 62(2): 315–329.

ANITA R GOHDES, b. 1986, PhD Candidate in Political Science, University of Mannheim (2011–); research interests: state repression, political violence, and human rights measurement; recent articles in *Journal of Conflict Resolution* and *Journal of Human Rights*.