Pulling the Plug: Network Disruptions and Violence in the Syrian Conflict*

Anita R. Gohdes
University of Mannheim

January 31, 2014

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 military offensives 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 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. The results indicate that such network blackouts constitute a part of the military's tactic to target and weaken opposition groups, where the underreporting of violence is not systematically linked to outages.

*Email: anita.gohdes@uni-mannheim.de. I thank Sabine Carey, Mike Colaresi, Bethany Lacina, Kathleen G. Cunningham, Jessica Maves Braithwaite, Will Moore, David Siegel, and the participants of the Workshop on Communication, Technology and Political Conflict at the University of Yale for helpful comments. All errors are my own.

"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 of 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 and York, 2012; Miller and Sienkiewicz, 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. Technical evidence on the trajectory of these outages suggests they were implemented in a way that could only have been conducted by the government (Cloudflare, 2012).[3]

Recent research has focused on the potential new technologies offer to opposition movements (Diamond and Plattner, 2012), but the logic and effect of these technologies being shut down again remains largely unclear. The fact that the current Syrian case is said to be 'the most socially mediated civil conflict in history (Lynch, Freelon and Aday, 2014, 5)' indicates the crucial role the internet is likely going to play in future conflicts. Understanding the motivation behind network manipulations instituted by regimes fearful of their political survival is therefore becoming increasingly indispensable for our theoretical and practical understanding of conflict dynamics, and learning from current cases such as Syria is an important place to start.

[1] Amal Hanano, journalist, on Twitter: https://twitter.com/AmalHanano/status/274169153781387265, 29. Novemer 2012.

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

[3] see Ars Technica: http://arstechnica.com/information-technology/2012/12/paint-it-black-how-syria-methodically-erased-itself-from-the-net/.

In this paper, I argue that governments fighting to maintain political control have an incentive to implement internet blackouts in conjunction with larger military offensives against opposition forces. Regime forces are likely to anticipate tactical advantages through shutting down virtual communication channels, in particular in regions of ongoing armed confrontation between pro- and anti-government forces, where the opposition has few alternative modes of accessing the internet. As such, the reduced opportunities for short-term military coordination of attacks is expected to improve government-aligned fighters' chances of regaining control. If shutting down all communication networks is perceived as a potential aid in repressing armed opposition groups, regime forces are likely to increase their military campaign against anti-government forces during outage periods. One observable consequence is therefore constituted by an increase in violence by regime supporters.

I empirically test this proposition using a new database 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 it 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 military

strategy, aimed at gaining operational advantages where the opposition is reliant on government-sponsored virtual communication channels. Whereas the partial cover-up of violence is likely to be a welcome side-effect for the regime, the evidence suggests that it does not constitute the primary goal of the network outages.

The rest of this paper is organized as follows. The next two sections review recent research on censorship 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 in light of being challenged by armed opposition groups. Following a discussion of possible alternative motivations, I formulate empirical expectations that can be tested to uncover the motivation behind implementing outages. The empirical section of this paper introduces the data on both regime violence and network outages in Syria, and then proceeds in presenting the results of the analysis of documented violence, and the variation in documentation patterns during outages. The paper 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 and Farquhar, 2012; Howard and Hussain, 2011; Tufekci and Wilson, 2012), less is known about how regimes facing such status quo challenges make use of these new technologies themselves. 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 (Aday, Farrell and Lynch, 2010, 20-21). Furthermore, SMS text-messaging was blocked during the entire election period (ibid.).

On the continuum of possible forms of media manipulation, unexpected implementation of internet and cell phone outages can be understood as an extreme form of government censorship against a country's own population. Howard and Hussain (2011) find that there were 556 recorded network outages between 1995 and 2011, with half of them occurring in authoritarian regimes. Their analysis suggests that while democratic governments generally shutdown 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 and Hussain, 2011, 225). There are plenty of recent examples that support these findings, such as the regimes in both Libya and Egypt that completely blocked their citizens' network access at the height of anti-government demonstrations in 2011 (Edmond, 2011, 1).[4] In September 2013, in the midst of anti-government protests sparked over fuel prices, Sudan disconnected 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. Furthermore, Burma's regime shut off all connections during 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 rebellion and protests.

However, existing evidence does not reveal to what extent such shutdowns are implemented in a concerted military effort to violently repress opposition groups, or whether they constitute a mere attempt to stop the outside world from following events on the ground. In this paper, I argue that in situations of extreme unrest, such as in the current Syrian civil war, network outages are used as a tactic to gain an advantage over the opposition in larger, short-term operations of repression.

[4] http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html

In other repressive contexts, governments have used more nuanced, proactive ways of censoring online content deemed hazardous to maintaining the status quo (see Deibert, 2008; MacKinnon, 2012; Rød and Weidmann, 2013). Deibert and 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 warantless 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 countries still making use of full disruptions are also the ones most afraid of political unrest erupting as a consequence of online communication (Deibert and Rohozinski, 2010, 28-29).

The risk of virtual communication inciting political unrest is corroborated by the behavior of other non-democratic governments, the largest being China. In the first large-scale quantitative analysis of social media censorship, King, Pan and 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 and Hollenbach (2013) find that locations with better access to wireless phone networks

display higher numbers of violent events.[5] 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 and Hollenbach, 2013, 210).

In contrast, Shapiro and Weidmann (forthcoming) 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 contradicting 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.[6] Possible adverse effects of total network outages for governments facing a discontented population are presented by Hassanpour (2013), who argues that a disruption can 'act[...] as a catalyst for the revolutionary process (Hassanpour, 2013, 1).' His evidence suggests that Mubarak's decision to briefly shut down the internet in 2011 was met by a dispersion and increase of demonstrators all across Egypt, making it increasing hard for the military to quell the protests.

From the position of the government, the availability of cell phone and internet connections can therefore be both boon and bane, providing both intelligence against the opposition and a space for coordination of the opposition at the same time. Decisions to obstruct these services are therefore likely to be made in strategic consideration of the costs and benefits associated with it.

[5] Shapiro and Weidmann (forthcoming) highlight potential issues with this finding: Violent events are equally more likely to be reported where communication is facilitated by mobile networks.

[6] Maintaining a neutral position in the face of conflict cleavages evidently poses a higher risk than taking a side (Kalyvas and Kocher, 2007), and in the face of increased communication flows on the ground, staying neutral might have become even harder.

Incentives for 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 outages? Faced with an already mobilized and violent opposition, large-scale network shut-downs are anticipated to decrease both the capability to successfully implement and the ability to coordinate attacks against the state.

Benefits of disruptions

The first anticipated benefit of shutting down network services pertains to the capability of opposition groups actually being able to implement effective attacks against the military. The recent civil wars in Libya as well as the ongoing Syrian conflict have both produced extensive footage of opposition fighters using online mapping services, such as Google Earth and Google Maps, to both accurately locate military targets and calibrate their weapons to effectively reach these targets (Miller, 2012; Brownstone, 2011; Keating, 2013). Faced with an army that is superiorly equipped with weapons, technology, and trained soldiers, opposition groups regularly find themselves in situations of asymmetric or 'irregular' warfare (Kalyvas and Balcells, 2010), where reliance on all available means of combat often constitute the only way of survival. Recent developments in the domain of geographical location systems made for personal use on devices such as smart phones and tablets therefore provide these groups with the capability of locating and targeting the military that would not have been as readily-available a decade ago.

Second, the ability to coordinate personell, material and strategies via mobile phones and the internet is a vital channel by which opposition groups are able to organize their rebellion. Compared to pre-internet days, the presence of virtual communication channels, in particular accelerated by the availability of smart phones, has increased the value of disseminating information and using it as a 'coordinating force [...] dramati-

cally' (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)', which means these tools are available to anyone with a working internet connection. Recent studies even report that social networking opportunities may in fact positively affect the political awareness of unsatisfied citizens (Reuter and Szakonyi, 2013), an attribute that is likely to increase the pool of potential recruits of anti-government rebellions (Tufekci and Wilson, 2012). The decentralized nature of the internet and social media thus offer the opposition 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 article 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 imminent threat posed by the increased abilities to coordinate, disseminate information, and even incite military soldiers to join the rebellion are likely to be clearly visible to authoritarian rulers in fear of their political survival. In a campaign aimed at repressing and possibly even eliminating the opposition, shutting down the most important coordination channel of the opponent is therefore a rational policy decision the government can pursue.

For a shutdown to effectively disrupt an opposition group's ability to coordinate and communicate, these channels must be available prior to - and in the aftermath of - a disruption. Longer periods without access to state-provided network services reduce any incentive to rely on these means of communication, and therefore increase the prob-

ability of rebel groups finding alternative means and services, such as satellite phones and modems, network access via neighbouring countries, or dial-up connections (when landlines are accessible).[7] Whereas sustained outages might impede on the long-term mobilization capacity of opposition groups dependent on rallying supporters via social media platforms, they might also motivate dissatisfied people to join protests against this extreme form of censorship. Outages that only last a couple of days or even less are going to affect same-day mobilization and last-minute coordination between opposition members, without burdening an entire population for too long.

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 that the usage of satellite mobile devices pertains a high risk as it produces traceable signals that allow governments to simply locate users and even trace their messages (see Driessen et al., 2012).[8] Given the relatively sparse usage of satellite phones, 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.[9] Although opposition groups might therefore possess

[7] 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.

[8] The topic of governments tracing opposition signals is relatively new, but news reports quoting researchers support this assumption:

> '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).

Furthermore, security researcher Jacob Appelbaum was quoted in an interview with the Electronic Frontier Foundation saying:

> 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 and Timm, 2012).

[9] The recent killings of two journalists in Homs in February 2012 support the suspicion 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 and Timm, 2012).

alternative ways of connecting via cell phone and internet, the increased usage of satellite devices is likely to improve the regime's capability of locating its desired targets. In the context of counterinsurgency offensives, the importance of identifying armed fighters among the civilian population is paramount (Valentino, Huth and Balch-Lindsay, 2004), and having these fighters identify themselves via satellite technology is likely to facilitate this task considerably.

Where state-run cell phone and internet services provided by the government are accessible, opposition groups are likely to make use of them. Shutting down these networks on an infrequent, unannounced basis is therefore likely to provide governments with an operational advantage, even in cases where rebel fighters resort to other networks.

Costs of disruptions

Shutting down network services, however, does not only affect opposition fighters and supporters, it affects a country's entire population. A major cost governments face when obstructing services concerns its economic revenues. When the Mubarak regime shut down its internet services for five days in 2011, the Egyptian economy lost an estimated $90 million worth of revenues (Howard and 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 shutdown of general communication services, such as those generated by tourism cites, call centers and e-commerce, as well as potential losses on investment in the aftermath of the blackout (see OECD, 2011).

A population that previously relied on the internet in both their personal and professional life is likely to be increasingly skeptical of a government that makes these channels unavailable to them. A recent study by Hassanpour (2013) finds 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. In the face of an armed opposition attempting to take over political authority, frequent and long outages can therefore be expected to weaken the capabilities of regimes fighting

for survival, both because of lost economic revenues and because of dwindling internal support through the population.

Lastly, governments pursuing a counterinsurgency strategy are highly dependent on information provided by the civilian population (Galula, 1964). Cell phone and internet access both considerably facilitate the means of communication for civilians willing and able to share crucial information on the location and activities of opposition fighters, without said fighter noticing the correspondence. Shapiro and Weidmann refer to this as the "'human intelligence" mechanism (Shapiro and Weidmann, forthcoming, 5)', which should ultimately provide the state with an advantage over the rebellion.

With economic revenue, human intelligence, and civilian support at stake, governments should therefore be wary of implementing large-scale internet shutdowns on a frequent or prolongated basis.

Given both the incentives and costs for governments in shutting down their networks, the negative consequences of cutting all connections are likely to be lowest if the outages are short, and the anticipated effects of weakening the opposition are likely to be strongest where outages occur on an irregular, unexpected basis. Prior knowledge of planned outages is likely to provide opposition groups with sufficient time to reorganize their means of coordination. Frequent usage of this tactic is also likely to decrease the benefits of relying on this mode of communication. Even worse, if network disruptions precede all forms of military actions and occur on a regular basis, opposition groups will be able to use this as an 'early-warning system'.

Cover-Up or Military Tactic?

An alternative explanation for shutting down network services in contentious situations could be the government's intention of covering up and hiding violent acts from international scrutiny. Contemporary conflicts are being documented and simultaneously shared with the outside world through the help of the internet (Diamond, 2010).

In situations 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 and Balch-Lindsay, 2004, 385) and eliminating the opposition, without creating a national and international audience that could potentially increase the risk of sanctions or interventions. Given the importance of mobile and virtual communication in disseminating and documenting evidence of human rights abuses, shutting down these channels might be perceived as an effective way to repress information flows.

This explanation has been supported by international advocacy groups, such as Amnesty International, who issued a statement in November 2012, saying 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'.[10]

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.

Testable Implications

If governments use network disruptions as a military tactic that forms part of a concerted repressive offensive against opposition groups, a main observable outcome is an increase in the activity of pro-government fighters during and in the immediate timespan surrounding outages. Larger military offensives require troops, material and weapons to be assembled and this process not occur on exactly the same day as the launching

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

of the additional 'network offensive'. For this reason, I expect increases in military activity coinciding and immediately preceding disruptions to indicate the military value governments ascribe to shutting down network services.

Pro-government fighter activity is measured by the number of people killed by the regime. According 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 number of *actual* people killed is defined as the combined number of *documented* and *undocumented* fatalities.[11] In order to understand whether disruptions are linked to higher levels of violence, it is crucial to account for changes in both the documented and the undocumented violence, since changes in communication technology might have an affect on the documentation process. The main empirical expectation, given that disruptions are part of a state's set of military tactics is:

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:

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 scenario that is possible is that governments

[11] 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.

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* with the violence once the networks are disconnected. Starting a campaign of violence and then shutting out the international community is likely 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 military tactic hypothesis.

[– Table 1 about here –]

Table 1 summarizes the expectation of the main hypotheses and the alternative explanation for documented violence, the % of undocumented violence, as well as 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 in 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 disconnections. These two types of disruptions differ profoundly in their nature and occurrence. This paper only analyzes large-scale national outages. First, there is strong evidence that confirms the large-scale outages to have been directly implemented by the Syrian government (Cloudflare, 2012). Second, news reports confirm that country-wide network outages are simultaneously accompanied by the disruption of cell phone services.[12] Third, these outages have occurred at irregular intervals, without being anticipated by either the international media or the opposition groups. For example, when on the 29th of November 2012 the third countrywide outage occurred,

[12] See, e.g. http://www.cbc.ca/news/world/syria-cuts-off-internet-cellphone-service-1.1133628, http://www.bbc.co.uk/news/technology-20546302, http://news.xinhuanet.com/english/world/2012-11/30/c_132008299.htm.

Western Media outlets voiced outrage and argued that 'it signaled the beginning of a dangerous new phase after 20 months of escalating conflict.'[13]

The second type of internet outage occurs at the regional level, where parts of the country that have been predominantly controlled by opposition groups, most notably the Northern governorates Ar-Raqqah and Al-Hasaka, have been cut off from the internet for most of the ongoing period under investigation. Syrian security experts contend that these cutoffs are implemented by the government 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.[14] Importantly, areas where government and opposition forces are fighting to win control are not affected by these outages.

Whereas the national-level blackouts can be viewed as short term 'shocks' to the ongoing conflict, evidence suggest that the duration and location of the local outages are highly endogenous to conflict dynamics, making it impossible to analyze the effect of both phenomena in the same framework. Since the country-wide blackouts fulfil the preconditions to be part of an effective military offence as presented above viz. previously accessible networks that are cut at irregular intervals by surprise, the effect of these disruptions will be investigated in this paper.

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.[15]. 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.[16] I include three different measures to account

[13]'Syria's Internet shutdown leaves information void, may signal escalating war', Washington Post, November 29, 2012: http://articles.washingtonpost.com/2012-11-29/world/35585439_1_syrian-people-hama-opposition-coalition

[14]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(https://syria.secdev.com/)

[15]http://www.google.com/transparencyreport/traffic/

[16]The fraction of normalized worldwide traffic in Syria in displayed for a sample of outages in the online appendix

for outages: First, a dummy variable that takes on the value of 1 on days where the traffic was disrupted, and a 0 for days of normal connection. The second accounts for the number of previous outages in order to test whether the effect increases or decreases over time. The third variable measures the time since the last outage, as recent outages might positively or negatively affect the dynamics of violence. To test for violence preceding disruptions, I code a dummy variable that take on 1 on days prior to disruptions, and 0 otherwise.

Documented Conflict Fatalities

In order to analyze the effect of country-wide network outages on violence, I make use of a newly assembled dataset that combines information on fatalities in Syria that were collected by five organizations that have been continuously working since the outset of the conflict.[17] In order to assure the highest possible quality standards in combining documented evidence from different sources, the dataset only includes records of fatalities that are identifiable by full name of the victim, date of death and governorate in which the death occurred. The records are therefore available at a daily level for each of the country's 14 governorates; further geographical disaggregation is not possible.[18] The five sources included in the analysis are the Syrian Center for Statistics and Research (SCSR)[19], the Syrian Network for Human Rights (SNHR)[20], the Syrian Observatory for Human Rights (SOHR)[21], the Syria Shuhada (SS) Website[22], and the Violations Documentation Centre (VDC)[23].

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,

[17] To my knowledge these are the only five organizations that have been continuously collecting data for the entire conflict period.

[18] Although the geographical information cannot be consistently assessed on an exact location-basis, the majority of records include further details on the circumstances of the incident, with some even providing links to videos portraying the deceased victims.

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

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

[21] http://syriahr.com/

[22] http://syrianshuhada.com/

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

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 a total number of uniquely documented victims. These procedures were conducted by Price et al. (2013)[24]. For the period from March 2011 to April 2013, Price et al. (2013) included 256,455 records from the five sources mentioned above into the record-linkage process, and arrive at a total number of 90769 uniquely documented victims.[25] For the period from May to September 2013 the dataset only includes linked fatalities from four sources.[26]

The data entail no detailed or consistent perpetrator information. However, all five sources publicly support the opposition, and their documentation processes focus on victims killed by the pro-government forces. All of the lists included in this analysis are classified as 'martyr' deaths by the recording groups, which means that regime deaths, such as military, paramilitary and other higher ranking officials are documented as being excluded from their databases. Although it is very likely that the documented killings examined in this analysis include a small proportion of victims killed by anti-government forces, the majority of cases are attributable to the regime.

[– Table 2 about here–]

Table 2 provides an overview of the documented daily fatality counts by governorate. The highest number of fatalities are reported in Rural Damascus, Homs, Aleppo and Idlib. Rural Damascus also witnessed the maximum number of fatalities per day for the period from March 2011 to September 2012, which more than doubles any other governorate. A closer look at the data reveal that the 645 uniquely idenfiable fatalities were recorded in Rural Damascus on the 21st of Augst 2013, the day of the chemical

[24] (for details, see Price et al., 2013, Appendix C)

[25] The number differs slightly from the total figure presented in Price et al. (2013) since the two data sources that only cover a part of the conflict were not included in this analysis. Furthermore, one of the excluded datasets comes from the Government of Syria and thus likely includes victims from within the regime, not victims killed by the regime.

[26] 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 five percent, making four source matching comparable to the previous period.

attack in the suburbs of Ghouta (UN, 2013). The outer governorates of Tartus, Ar-Raqqah, Al-Hasaka, Quneitra and As-Suwayda all have comparatively low numbers of documented violence, which is not surprising as these areas have not been at the center of clashes between regime and opposition forces for most of the conflict period under investigation (Holliday, 2013). In the absence of consistent struggles between the government and opposition, the expectation is that the effect of network outages is likely to be less pronounced than in governorates such as Rural Damascus, Aleppo, Homs and Idlib. Notably, Tartus witnessed at least one day of intense clashes, including the 2nd of May 2013, where the data suggest that 125 people were documented to have been killed, most probably in al-Bayda and Baniyas. The overall reported death toll in this Western governorate remained relatively low until September 2013.

Results: Network Outages and Documented Killings

I analyze the effect of network outages on documented daily killings by governorate in Syria. The descriptive difference 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 anti-government groups have almost established parallel government structures and have be excluded from the national network for large parts of the conflict (MacFarquhar and Saad, 2012), no discernible difference is to be found. Evidently, where the internet was never working, sudden national blackouts are not going to have an effect. 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, when compared to other days during the period under investigation. The conflict centers of Rural Damascus and Homs in the center of the country show average increase of more then 30 fatalities. The descriptive differences thus display a general trend that is in line with the empirical expectations.

[– Figure 1 about here –]

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 April to August 2011, marking the disruption days in June in red. 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 rise dramatically on the day *before* the blackout, decrease on the day to a nevertheless high number, and increase 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 military offensive need not necessarily be implemented prior to the commencement of fighting. Shutting down the network amidst fighting is likely to also constitute a role in a military strategy.

[– Figure 2 about here –]

With regional daily data from the 15th of March 2011 until the 30th of September 2013, I estimate a time-series cross section fixed-effects poisson model, where the 14 governorates are the fixed units and there are 931 time points for each of these units. The first model in Table 3 presents the results for the effect of network disruptions on governorate-level daily documented violence. Days where the entire country is disconnected are highly significantly associated with higher levels of documented violence. The variable counting the days since the last outage (Last Disr) is negatively associated with violence, suggesting that there is no general increase in violence between disruptions. Lastly, the number of previous disruptions (# Disr) does not seem to be associated with higher or lower levels of violence.

Since the regression results of poisson models cannot be interpreted in a straightforward way, 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 red lines show the expected change on the day of network outages, and the black 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 are significantly affected by violence all across Syria. 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 (red lines) experience on average three additional incidences of lethal violence when compared to days with regular access. The violent effect of network outages seem less pronounced in peripheral regions such as As-Suwayda, Al-Hasaka and Quneitra. Given the fact that these governorates on average witness one or less fatalities per day, the effect is nevertheless substantial.

[–Table 3 about here –]

[–Figure 3 about here –]

Turning to the model estimating the occurrence of violence on the days prior to disruptions, the expected changes 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 military tactic argument: Governorates in Syria experience a significant increase in conflict deaths perpetrated by the regime on days where the regime shuts down network services. Furthermore, a first substantial increase in violence seems to already be occurring one day prior, an increase we would not expect if the regime were interested in covering up atrocities during blackouts.

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 now only reports the change in fatalities between time t and t-1. The first model in Table 4 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 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 lastly, there seems to be no enduring effect once networks are turned back on again.

[–Table 4 about here –]

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 document violence. As in all conflicts, however, it is impossible to determine the universe of conflict fatalities through 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 paper, 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 (see Davenport and Ball, 2002). This study is no different, and the cover-up hypothesis even supports this claim. Violence might have been covered up during blackouts due to the reduced availability of online and cell phone communication.

One way to test for the cover-up hypothesis is to determine whether the level of underreporting differed substantially on days without internet when 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 1, 2, 3 or 4 sources can be used to estimate the number of fatalities that weren't documented by any source. Log-linear capture-recapture estimation follows this simple intuition and has been used to estimate fatalities in a multitude of conflicts (Zwierzchowski and Tabeau, 2010; Lum et al., 2010; Brunborg, Lyngstad and Urdal, 2003).[27] I isolate the number

[27]Log-linear poisson models for capture-recapture estimation are implemented in the R package Rcapture (see Baillargeon and Rivest, 2007). I choose log-linear models because they are effective at

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 both time and space, I select the fixed period of a month prior to each network disruption and estimate the level underreporting 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 disconnected days are systematically underreporting violence or not.

For example, during the internet blackout on the 3rd and 4th of June 2011, 104 victims were documented in Hama. Only 25 of these victims are reported in all lists, the remaining were reported by a combination of less than all sources.[28] Capture-recapture estimation reveals that it is highly likely that 123 individuals were killed in this period[29], which means that 15.4 % of all victims went undocumented in those two days. In the month prior to the June outage, 48 victims of regime violence were documented in Hama, of which only 4 were known by all sources. The estimated number of actual regime fatalities is 72, which means that 33.3% of all cases went undocumented. Figure 4 shows the relationship between undocumented fatalities prior and during network outages, where the x-axis is the % of undocumented fatalities in the month prior to the outage, and the y-axis shows the % of undocumented cases during network disruptions. In order to uncover possible regional stratifications, the points are labeled by the governorate they represent.

[– Figure 4 about here –]

If the degree of underreporting was always the same before and during outages, all observations would be aligned along the diagonal of the plot, where x=y. If documen-

dealing with capture heterogeneity and list dependencies, both of which are the main challenges when estimating conflict fatalities (see Manrique-Vallier, Price and Gohdes, 2013).

[28]With four sources, there are $2^4 - 1 = 15$ possible combinations of documentation.

[29]The point estimate arrives at a number of 19 undocumented fatalities, with bootstrapped 95% confidence intervals of [8,47]. Adding the documented number, the estimated total number of fatalities is 123 [112, 151], and an underregistration rate of 15.4%.

tation during outages were systematically displaying a higher number of undocumented cases (cover-up hypothesis), then most observations should be clustered in the top left corner of the plot. As expected, documentation rates prior to and during disruptions are positively correlated. No systematic underreporting during disruptions is however discernible. Additionally, the documentation rates do not seem to cluster substantially by governorate. The results presented in Figure 4 suggest that documentation patterns are not systematically linked to network outages. Whereas substantial variation in reporting is 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 (see Rød and Weidmann, 2013; Morozov, 2012). 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 of 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 substantially high increases 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 paper 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 paper's findings: the fact that undocumented violence in Syria is not systematically affected by short disruptions offers important support for the military tactic hypothesis.[30] Estimating the degree of underreporting however also demonstrates the high variability in documentation. Cases where more violence is hidden from view during disruptions might be a somewhat welcome side-effect for governments seeking to maintain international legitimacy and internal control.

This paper has attempted to understand why governments might have an incentive to include the disruption of internet and cellphone service into their military strategy. Whereas I have argued that the scarce and sudden disconnection from essential communication networks is likely to weaken opposition groups' propensity to organise, 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. Furthermore, this analysis has investigated the effects of nation-wide outages, additional research is needed to understand the logic of regional variations in network accessibility.

As mentioned in the introduction, Syria presents the first conflict that has been meticulously followed and fuelled by an online audience: by the opposition fighters and supporters, by regime forces and supporters, and by the outside world. The increasing importance of establishing control over both content on and access to the internet, is likely to exercise an increasing appeal on regimes intent on adjusting their repertoire of repressive tools to deal with these new digital threats to their stability.

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

References

Aday, Sean, Henry Farrell and Marc Lynch. 2010. "Blogs and Bullets: New media in contentious politics." *US Institute of Peace* .

Amnesty International. 2012. "Syria: Shutting down of internet and mobile networks alarming development." Press Release.
URL: *http://www.amnestyusa.org/news/press-releases/syria-shutting-down-of-internet-and-mobile-networks-alarming-development*

Baillargeon, Sophie and Louis-Paul Rivest. 2007. "Rcapture: Loglinear Models for Capture-Recapture in R." *Journal of Statistical Software* 19(5):1–31.
URL: *http://www.jstatsoft.org/v19/i05*

Breuer, Anita, Todd Landman and Dorothea Farquhar. 2012. "Social Media and Protest Mobilization: Evidence from the Tunisian Revolution." *Available at SSRN 2133897* .

Brownstone, Andy. 2011. "Meet the Libyan rebels on the front line." BBC News.
URL: *http://www.bbc.co.uk/newsbeat/13505340*

Brunborg, Helge, Torkild Hovde Lyngstad and Henrik Urdal. 2003. "Accounting for genocide: how many were killed in Srebrenica?" *European Journal of Population/Revue européenne de démographie* 19(3):229–248.

Cloudflare. 2012. "How Syria Turned Off the Internet.".
URL: *http://blog.cloudflare.com/how-syria-turned-off-the-internet*

Davenport, Christian and Patrick Ball. 2002. "Views to a Kill: Exploring the Implications of Source Selection in the Case of Guatemalan State Terror, 1977-1996." *Journal of Conflict Resolution* 46(3):427–450.

Deibert, Ronald. 2008. *Access denied: The practice and policy of global internet filtering.* MIT Press.
URL: *http://site.ebrary.com/lib/unimannheim/docDetail.action?docID=10214159*

Deibert, Ronald and Rafal Rohozinski. 2010. Control and subversion in Russian cyberspace. In *Access controlled: The shaping of power, rights, and rule cyberspace.* MIT Press Cambridge, MA pp. 15–34.

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

Diamond, Larry and Marc F Plattner. 2012. *Liberation technology: Social media and the struggle for democracy.* Johns Hopkins University Press.

Driessen, Benedikt, Ralf Hund, Carsten Willems, Christof Paar and Thorsten Holz. 2012. Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards. In *Security and Privacy (SP), 2012 IEEE Symposium on.* IEEE pp. 128–142.

Edmond, Chris. 2011. Information manipulation, coordination, and regime change. Technical report National Bureau of Economic Research.

Galula, D. 1964. *Counterinsurgency warfare: theory and practice.* Praeger Security International.

Hassanpour, Navid. 2013. "Media Disruption and Revolutionary Unrest: Evidence from Mubarak's Quasi-Experiment." *Political Communication* 30:1–24.

Holliday, Joseph. 2013. "The Assad Regime: From Counterinsurgency To Civil War." *The Institute for the Study of War* .

Howard, Philip N. and Muzammil M. Hussain. 2011. "The Role of Digital Media." *Journal of Democracy* 22(3):35–48.

Kalyvas, Stathis and Laia Balcells. 2010. "International System and Technologies of Rebellion: How the End of the Cold War Shaped Internal Conflict." *American Political Science Review* 104:415–429.

Kalyvas, Stathis and Matthew A. Kocher. 2007. "How" Free" Is Free Riding in Civil Wars?: Violence, Insurgency, and the Collective Action Problem." *World Politics* 59(2):177–216.

Keating, Joshua. 2013. "Firing Mortars? There's an App for That." Slate, 18 September.
URL: *http://slate.me/1mWnVcm*

King, Gary, Jennifer Pan and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107:1–18.

Lum, K., M. Price, T. Guberek and P. Ball. 2010. "Measuring Elusive Populations with Bayesian Model Averaging for Multiple Systems Estimation: A Case Study on Lethal Violations in Casanare, 1998-2007." *Statistics, Politics, and Policy* 1(1):2.

Lynch, Marc, Deen Freelon and Sean Aday. 2014. "Blogs and Bullets III: Syria's Social Mediated War." *US Institute of Peace* .

MacFarquhar, Neil and Hwaida Saad. 2012. "Rebel Groups in Syria Make Framework for Military.".

MacKinnon, Rebecca. 2012. *Consent Of The Networked: The Worldwide Struggle For Internet Freedom*. Basic Books.

Madory, Doug. 2013. "Internet Blackout in Sudan.".
URL: *http://www.renesys.com/2013/09/internet-blackout-sudan/*

Manrique-Vallier, Daniel, Megan E Price and Anita Gohdes. 2013. Multiple Systems Estimation Techniques for Estimating Casualties in Armed Conflicts. In *Counting Civilian Casualties: An Introduction to Recording and Estimating Nonmilitary Deaths in Conflict*. Oxford University Press pp. 165–182.

Miller, Elhanan. 2012. "Syrian opposition uses home-made rockets and Google technology, video reveals.".
URL: *http://www.timesofisrael.com/syrian-opposition-uses-home-made-rockets-google-technology-new-video-reveals/*

Miller, James and Matt Sienkiewicz. 2012. "Straight news from the citizens of Syria How reporters sort, organize—and verify—a flood of information from a chaotic civil war." *Columbia Journalism Review* .

Morozov, Evgeny. 2012. *The net delusion: The dark side of Internet freedom*. PublicAffairs Store.

OECD. 2011. "The economic impact of shutting down Internet and mobile phone services in Egypt.".
URL: *http://bit.ly/1ehhDmB*

OpenNet Initiative. 2009. Internet Filtering in Syria. Technical report.

Perlroth, Nicole. 2013. "Syria Loses Access to the Internet.".
URL: *http://nyti.ms/1cu5jzd*

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

Pierskalla, Jan H. and Florian M. Hollenbach. 2013. "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa." *American Political Science Review* 107:207–224.

Price, Megan, Jeff Klingner, Anas Qtiesh and Patrick Ball. 2013. "Updated Statistical Analysis of Documentation of Killings in the Syrian Arab Republic." *Human Rights Data Analysis Group* .

Reuter, Ora John and David Szakonyi. 2013. "Online Social Media and Political Awareness in Authoritarian Regimes." *British Journal of Political Science* FirstView:1–23.

Rød, Espen Geelmuyden and Nils B. Weidmann. 2013. "Empowering Activists or Autocrats? Internet and Authoritarian Survival." *Working Paper* .

Shapiro, Jacob N and Nils Weidmann. forthcoming. "Is the Phone Mightier than the Sword? Cell Phones and Insurgent Violence in Iraq." *International Organization* .

Shirky, Clay. 2008. *Here comes everybody: The power of organizing without organizations*. Penguin.

Tufekci, Zeynep and Christopher Wilson. 2012. "Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square." *Journal of Communication* 62(2):363–379.
URL: *http://dx.doi.org/10.1111/j.1460-2466.2012.01629.x*

UN. 2013. "Report on the Alleged Use of Chemical Weapons in the Ghouta Area of Damascus on 21 August 2013.".

Valentino, B., P. Huth and D. Balch-Lindsay. 2004. "Draining the Sea: Mass Killing and Guerrilla Warfare." *International Organization* 58(02):375–407.

York, Jillian and Trevor Timm. 2012. "Satphones, Syria, and Surveillance.".
URL: *https://www.eff.org/deeplinks/2012/02/satphones-syria-and-surveillance*

Youmans, William Lafi and 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.
URL: *http://dx.doi.org/10.1111/j.1460-2466.2012.01636.x*

Zwierzchowski, Jan and Ewa Tabeau. 2010. The 1992-95 War in Bosnia and Herzegovina: Census-Based Multiple Systems Estimation of Casualties' Undercount. Conference Paper for the International Research Workshop on 'The Global Costs of Conflict'.

Figures and Tables

Figures

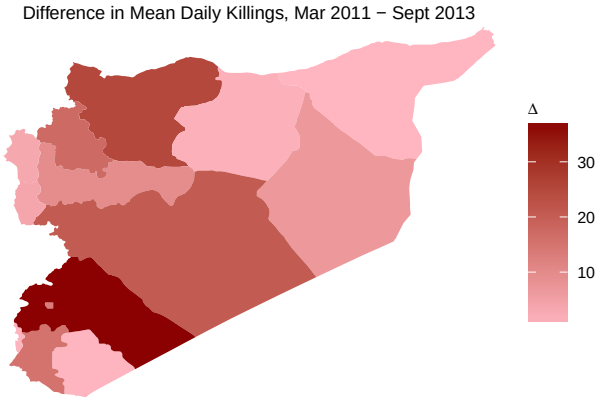
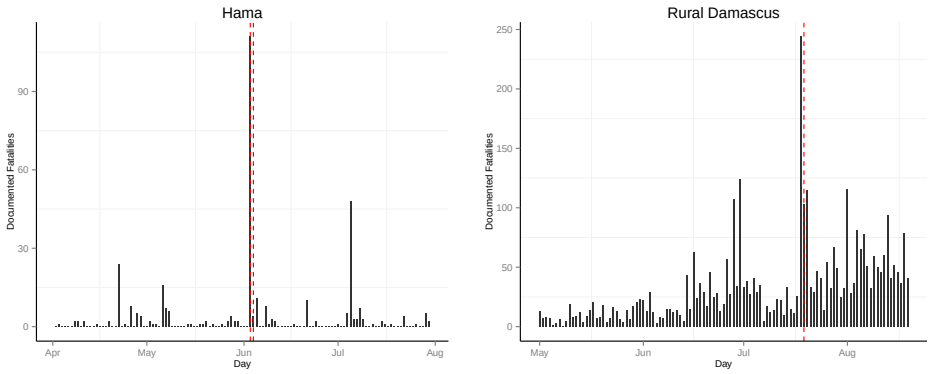


Figure 1: Mean Difference in Daily Killings between Days with and without internet



(a) Hama 2011 (b) Rural Damascus 2012

Figure 2: Violence and Network Disruptions

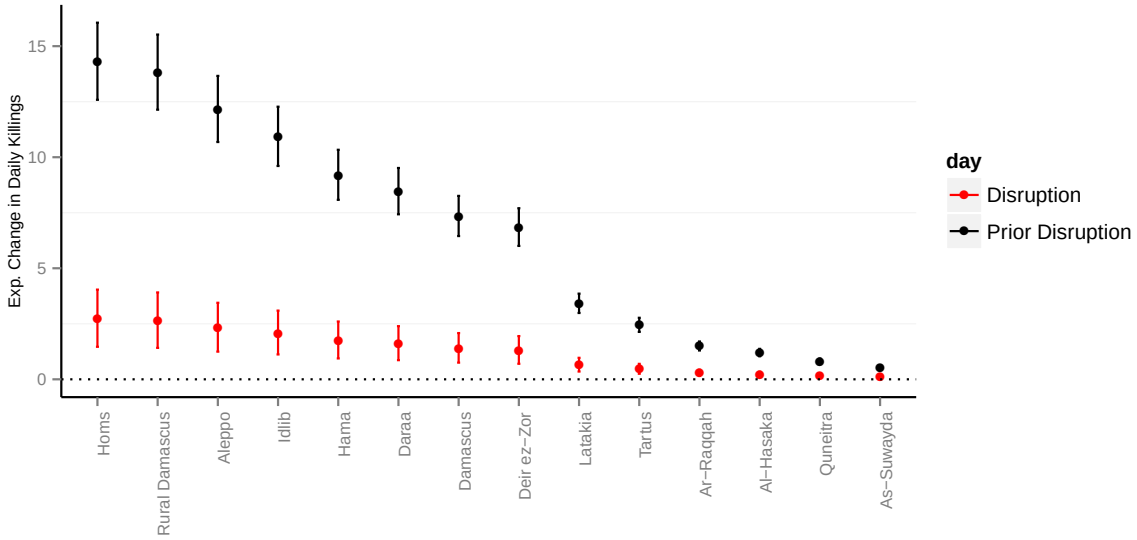


Figure 3: Expected Change in Daily Killings, given Network Disruptions

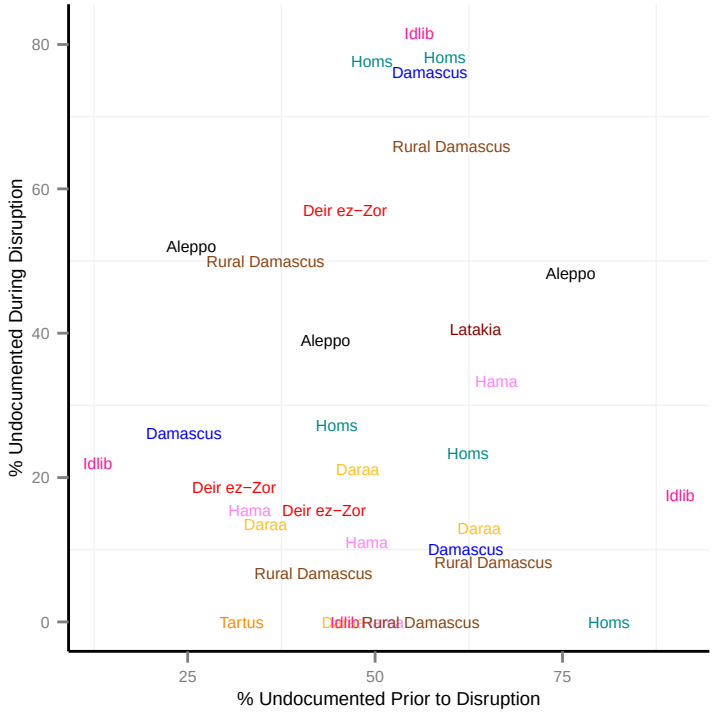


Figure 4: % of Undocumented Fatalities Prior and During Disruptions

Tables

Expectation	**Documented**	**% Undocumented**	**Timing**
Military Strategy	increase	no change	prior/ during disruption
Cover-Up	no change / increase	increase	*only* during disruption
No Effect	no change	no change	

Table 1: Expected Effects for Network Disruptions and Violence

Governorate	min	max	mean	sd	sum
Rural Damascus	0	645	24	34	22155
Homs	0	265	19	20	17823
Aleppo	0	255	16	19	14665
Idlib	0	164	13	14	11831
Daraa	0	185	11	13	9898
Hama	0	168	10	13	9100
Damascus	0	137	8	12	7622
Deir ez-Zor	0	117	7	10	6472
Latakia	0	66	3	5	3203
Tartus	0	125	3	6	2413
Ar-Raqqah	0	29	2	3	1458
Al-Hasaka	0	31	1	3	1141
Quneitra	0	42	1	2	786
As-Suwayda	0	8	0	1	433

Table 2: Summary Statistics, Documented Fatality Counts

	Disruption	Pre Disr	Window
(Intercept)	0.265^{***}	0.262^{***}	0.252^{***}
	(0.034)	(0.034)	(0.034)
Disruption	0.154^{***}		
	(0.034)		
Pre Disr		0.630^{***}	
		(0.029)	
Time Window			0.310^{***}
			(0.018)
Last Disr	-0.001^{***}	-0.001^{***}	-0.001^{***}
	(0.000)	(0.000)	(0.000)
# Disr	0.014	0.052^{***}	-0.022^{*}
	(0.012)	(0.008)	(0.009)
Viol_{t-1}	0.008^{***}	0.008^{***}	0.008^{***}
	(0.000)	(0.000)	(0.000)
Viol_{t-2}	0.008^{***}	0.008^{***}	0.008^{***}
	(0.000)	(0.000)	(0.000)
...	...	...	...
BIC	108872.44	108501.99	108631.62
Log Likelihood	-54348.74	-54163.52	-54228.33
Deviance	82101.11	81730.66	81860.29
Num. obs.	9982	9982	9982

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{+}p < 0.1$

Poisson Regression. Governorate Fixed Effects not displayed.

Disr: Network Disruption

Table 3: Network Disruptions and Violence

	Pre Disr	First Day	Post Disr
(Intercept)	$-0.325^{\cdot}$	-0.013	-0.304
	(0.185)	(0.012)	(0.187)
Pre Disr	5.740^{***}		
	(1.418)		
First Day		0.373^{+}	
		(0.197)	
Post Disr			1.172
			(1.428)
Last Disr	0.002^{*}	0.000	0.002^{*}
	(0.001)	(0.000)	(0.001)
# Disr	0.409	-0.026	0.404
	(0.334)	(0.050)	(0.334)
Diff_{t-1}	-0.593^{***}	-0.020^{***}	-0.594^{***}
	(0.010)	(0.001)	(0.010)
Diff_{t-2}	-0.251^{***}	-0.009^{***}	-0.251^{***}
	(0.010)	(0.001)	(0.010)
R^2	0.275	0.091	0.274
Adj. R^2	0.275	0.091	0.274
Num. obs.	9982	9982	9982

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, $^{+}p < 0.1$

Table 4: First Difference Model: Network Disruptions and Changes in Violence

A Online Appendix

Network Disruptions on Google

Graphs were created and copied from https://www.google.com/transparencyreport/traffic/. All rights belong to Google.

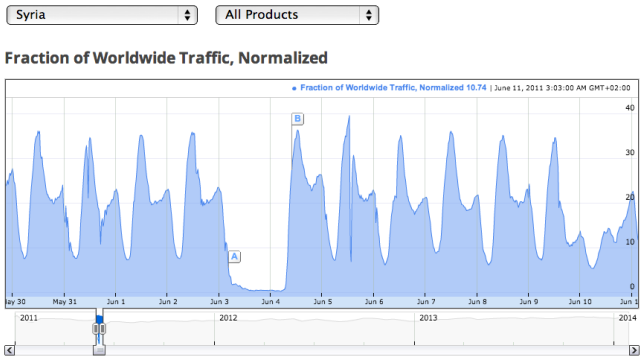


Figure A1: Disrupted Google Traffic, June 2011

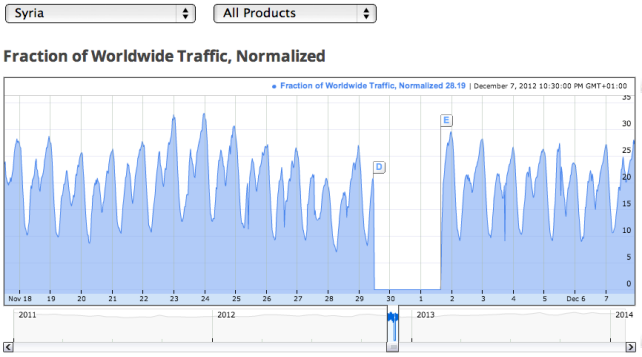


Figure A2: Disrupted Google Traffic, Nov/Dec 2012

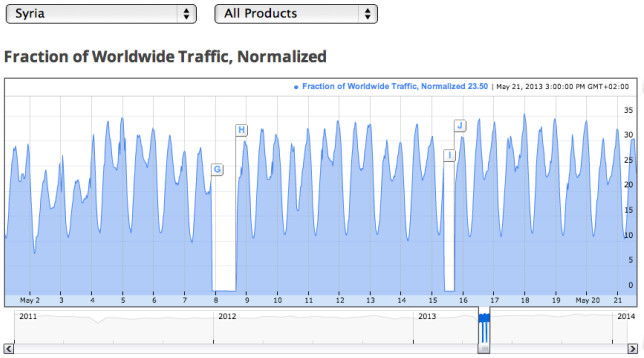


Figure A3: Disrupted Google Traffic, May 2013