Repression technology: Internet accessibility and state violence

Anita R. Gohdes*
Hertie School of Governance

March 13, 2019

Abstract

This article offers a first subnational analysis of the relationship between states' dynamic control of Internet access and their use of violent repression. I argue that where governments provide Internet access, surveillance of digital information exchange can provide intelligence which enables the use of more targeted forms of repression, in particular in areas not fully controlled by regime. Increasing restrictions on Internet accessibility can impede opposition organization, but limits access to information on precise targets, resulting in an increase in untargeted repression. I present new data on killings in the Syrian conflict that distinguish between targeted and untargeted events, using supervised text classification. I find that higher levels of Internet accessibility are associated with increases in targeted repression, whereas areas with limited access experience more indiscriminate campaigns of violence. The results offer important implications on how governments incorporate the selective access to communication technology into their strategies of coercion.

*Previous versions of this paper have been presented at the New Faces in Political Methodology VIII Conference at Penn State University, the APSA Annual Meeting in Washington DC, the ISA Annual Convention in New Orleans, and the 31st Chaos Communication Congress in Hamburg. For excellent comments I thank Pablo Barberá, Sabine Carey, Dara Cohen, Chris Fariss, Stathis Kalyvas, Jason Lyall, Will Lowe, Kelly Greenhill, Will Moore, Nils Weidmann, as well as participants of the International Relations Workshop at Yale, the USC Networked Democracy Lab, the Belfer Center International Security Seminar, the Conflict, Security, and Public Policy Workshop at the Harvard Kennedy School, as well as at ETH Zurich, Duisburg, and Uppsala University.

Introduction

The ability to connect via large social network platforms has been celebrated by social scientists, policy makers, and human rights groups across the world as an empowering new way for ordinary citizens to collectively mobilise against repressive rulers. Amidst the civilian uprisings that spread like wildfire across the Middle East and North Africa in 2011, social media was declared the principal tool of the protest movement, with journalists and researchers proclaiming that in the twenty-first century, 'the revolution will be tweeted' (Hounshell, 2011). In consequence, the opportunities offered by the digital media to previously marginalised voices of dissent, and the role they play in facilitating protest and resistance, have become the subject of extensive research (see Tufekci, 2017; Steinert-Threlkeld, 2017). Next to the euphoric accounts of the digital revolution there is, however, increasing evidence that shows how behind the scenes, governments across the world have been continuously developing and refining a whole arsenal of tools to surveil, manipulate, and censor the digital flow of information in the realm of their authority (see Roberts, 2018; Deibert et al., 2010).

This article investigates to what extent Internet restrictions are part of larger repressive campaigns instigated by governments set on maintaining political control. I argue that increased use of social media presents governments who fear for their political survival with a dilemma. On the one hand, dissidents and opposition groups are empowered through the use of social media; on the other hand these platforms offer themselves to previously unseen levels of surveillance and manipulation. States face a trade-off: the more they restrict access to the Internet and with it diminish opposition groups' capabilities, the less they are able to monitor digital exchange of information to their own advantage. Vice versa, increased Internet access offers opportunities to surveil potential challengers, but simultaneously provides the digital infrastructure for opposition groups to organize and develop their capabilities. Strategies of Internet control can be situated along a continuous dimension ranging from full censorship on the one side to uncensored access and active surveillance on the other side.[1]

[1]The level of sophistication with which surveillance and censorship is conducted varies profoundly (Deibert et al., 2010), and some countries, such as China, invest substantial resources to first surveil and then censor information being exchanged by their citizens (see King, Pan and Roberts, 2013). However, the choice to, and extent of, censoring remains highly relevant for all governments, as overly

I argue that the choice of Internet control inevitably *limits* the use of some forms of violence and *enables* the use of other forms. *Digital surveillance* operations - which require a certain level of Internet access - provide highly specified intelligence on the intentions and location of opposition leaders, which should in turn enable governments to use *targeted violence*. Increased censorship - which in turn removes access to information - severely limits the choices for violent action on the side of the government, by censoring its own access to intelligence on precise targets. In areas and during times of increased censorship, state-sanctioned violence is likely to affect the domestic population *indiscriminately*. However, this relationship is mediated by local conditions that determine whether Internet controls will be more or less useful than more traditional forms of control.

To empirically test my argument, I turn to the Syrian conflict, where I analyze how subnational variations in Internet accessibility affect the regime's use of repressive strategies, looking at the period from June 2013 to April 2015. The Syrian conflict is one of the first conflicts where lines between online and offline conflict engagement have become blurred. From the outset of the conflict, digital media and communication has played a central role in both the regime's and the anti-government groups' strategies of contestation. The Syrian government has a demonstrated history of using telecommunications to spy on its own population, and with the introduction of social media in Syria, expanded its control of networks to this new form of communication. Likewise, it has, at different points in time, limited regional accessibility to the Internet across the entire country.

I present new data on killings by the regime and use text classification via supervised machine-learning to categorize over 65,000 observed records into targeted and untargeted acts of violence. To account for unreported events, I estimate actual levels of violence using multiple recapture estimation. I find that higher levels of information accessibility are associated with a substantive increase in both the proportion and absolute scale of targeted repression, whereas areas with little or no access witness more indiscriminate campaigns of violence. The increase is particularly pertinent in areas where the regime cannot rely on traditional networks of control, such as areas outside of their ethnic strongholds. The empirical analysis accounts for a range of important confounders, different measures of

ambitious restrictions have the potential for provoking self-censorship (Roberts, 2018) or inciting unrest (Hassanpour, 2014).

Internet accessibility, and a variety of different model specifications. The findings highlight the ambiguos role digital technologies play in contentious settings, providing low-cost coordination mechanisms for challengers, but equally informing governments' repressive strategies in previously unexplored ways.

Broadening the repressive toolkit in the digital age

Governments intent on maintaining power over all adversaries have long combined the use of information control and restriction with the use of violence against those deemed threatening to their authority (Van Belle, 1997). Traditionally, more extreme forms of controlling information have been implemented by banning newspapers, radio and television stations, and targeting journalists (Whitten-Woodring, 2009). Less extreme forms have included the surveillance of news agencies, as well as banning and alteration of individual media content. Overly zealous restriction has the potential of backfiring, where citizens rate the absence of reporting as 'bad news' (Shadmehr and Bernhardt, 2012, 26), and thus lower their support for the ruling elite. Conversely, leaders fear that free and public criticism of their policies might jeopardize their standing even more. The rise of citizen journalists working independently of traditional news agencies and sharing content via Internet platforms has changed the dynamics and tools used by both state and opposition forces considerably (Aday, Farrell and Lynch, 2010). Information shared via the Internet poses a particular threat to governments as it is harder to control both the content producers and consumers, and it spreads information considerably faster than traditional media. At the same time, the decentralized nature of the Internet has broadened the repertoire of surveillance and infiltration for governments (Morozov, 2012).

The toolbox of instruments that states can use to repress their citizens has broadened with the rise of digital media and communication technology. Governments now have the option of controlling whether and in what form citizens are able to connect online, as well as the ability to extensively surveil online communication (MacKinnon, 2012). However, so far there has been a lack of research on how the state's use of violence is affected by these changes, despite the fact that there has been ample research demonstrating how the dramatic increase in collective organization via social media platforms has made states

more susceptible to both internal protest and dissent (Earl and Kimport, 2011; Pierskalla and Hollenbach, 2013).

While state control of the Internet is widespread, the methods used vary widely (Gunitsky, 2015; Deibert et al., 2010). Deibert et al. (2010) contend that while early digital controls - practised in countries such as Uzbekistan, Turkmenistan, the United Arab Emirates, and Saudi Arabia - involved the consistent blocking of websites, governments now make use of more dynamic, case-specific restrictions that are only used in response to changes in the political and social environment. Such controls are often implemented under the pretense of national security and implemented dynamically when and where the state perceives itself to be under imminent threat, such as during protests, strikes, or in post-election periods (Deibert et al., 2010, 24-25). 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), so as to avoid growing unrest. In Syria, country-wide shutdowns generally coincide with more intense government violence, indicating that they are employed to strategically weaken the coordination capabilities of the opposition (Gohdes, 2015). Research on China shows that significantly more content inciting collective organization is removed than other content, even when it is explicitly criticising the ruling party (King, Pan and Roberts, 2013).

The majority of research dealing with Internet controls in the context of contentious politics has focused on how Internet restrictions might quell or instigate unrest and rebellion (Kalathil and Boas, 2003; Little, 2016). In the context of violent state repression, the benefits of *refraining* from Internet restrictions to surveil the exponential increase in user-generated content via the Internet have remained largely under-studied (MacKinnon, 2012). Although the use of surveillance to facilitate targeted arrests and elimination of threats to the political survival of regimes has long since been a part of the repertoire of coercive tools used by governments, the Internet has radically facilitated and reduced the costs of mass surveillance (Deibert, 2003). For example, in the pre-Internet era, even state authorities known for their meticulous approach towards mass surveillance, such as the German *Staatssicherheit* in the German Democratic Republic, were constrained by technological and human capacity limits when listening in on phone calls, positioning staff in next-door homes, and getting neighbours, family and friends to spy on each other.

Surveillance via the Internet offers a multitude of new opportunities for governments who are fearful for their political survival. Merely providing improved communication networks can already facilitiate the sharing of information on the location and planned activities of dissidents or insurgents (Shapiro and Weidmann, 2015). But many governments employ modern tools that allow them to intercept information exchanged via social media. Such information and the corresponding meta-data can help identify those deemed most threatening, and it also reveals information about friends, followers and fellow activists who are most likely to sympathise with the opposition's actions and beliefs (Marczak et al., 2014). Autocratic regimes increasingly also make use of social media channels to enforce their own political and social agenda (Gunitsky, 2015), divert attention (King, Pan and Roberts, 2017), and discredit opponents (Tufekci, 2017). Importantly, Internet accessibility is a precondition for these tactics to work.

Digital controls and state violence

I argue that restricted network access is likely to go hand in hand with broader, more indiscriminate campaigns of state violence. In contrast, maintaining network connections in order to digitally surveil citizens can support regimes in identifying specific, individual threats, and therefore will be associated with more targeted repressive campaigns.

The two policy options available to governments that are under consideration here, are the use of Internet controls and the use of violent state coercion. I assume that a repressive strategy is chosen if government actors expect it will help eliminate or at least mitigate the threat posed, for example, by an insurgency, mass uprising or even smaller-scale protest. Ideally, such a strategy would involve identifying those individuals or organizations that are genuinely challenging, or in favor of challenging, the authority's position and eliminating them, for example through arrest, expulsion, disappearance, or even violent death. To do this, leaders need identifying information (Shapiro and Weidmann, 2015; Kalyvas, 2006).

Freely accessible digital communication channels provide governments with a means of digital surveillance, which can be used to identify perceived central threats with higher

levels of details and accuracy. The main tradeoff involved is that for surveillance to work, critical information needs to be exchanged, which in turn can further strengthen the ties of those opposed to the government. For example, the Iranian government limited Internet access during the national elections in 2009, while both Turkey and China have blocked individual social media accounts during mass protests. These policies aim at restricting criticism and calls for collective organization, in order to maintain control and stability. However, stability comes at the price of information loss (Lorentzen, 2013).

Surveillance facilitates targeted violence

In order for government actors to employ digital surveillance tools, the targeted population needs to have access to the Internet. Where citizens freely converse with others online, they generate vast amounts of information that can be used to create nuanced models of interaction, perceptions, location, intention, and network of collaborators for each citizen (Lyon, 2009). Public and private events organized and distributed via social media, email, and other channels can easily be anticipated, and prospective participants predicted and placed under even closer surveillance. Each individual's *friends*, *followers*, call logs, newsletters, subscriptions and text messages can be used to obtain an understanding of how resistance movements are organized, and who constitutes the central actors. Once these particular 'threats' are identified, location-based services can aid in isolating and targeting them.

The data gleaned from tracking online conversations can help identify dissidents in an early and precise way, providing governments with an opportunity to target dissidents who have either organized dissident activities in the past, or plan are planning future events. When opposition activities do erupt, surveilling the entire population's response to it can help anticipate the potential for future rebellion and assess how such activities affect public opinion. Surveilling known dissidents' devices can help identify networks of opposition groups, including their location, their supporters' locations, as well as their means of accessing material support (Marczak et al., 2014).

The collection of highly specified intelligence on the intentions and location of critical players in anti-government movements enables state violence to be more targeted and

tailored towards individuals (Galperin, Marquis-Boire and Scott-Railton, 2013). Digital surveillance during full Internet accessibility is therefore likely to increase states' use of targeted, individualised violence against domestic threats. *I therefore expect that, all else equal, government provisions for the free exchange of information are likely to be positively associated with a targeted coercive response tactic.*

Untargeted violence in the face of censorship

Disrupting full or partial access to the Internet is, from a technical standpoint, low-cost, and quick to implement. Temporary digital restrictions can be excused as technical failures, giving governments, at least for a short time, the possibility to plausibly deny active involvement. Responsibility is particularly easy to deny in situations where access is not fully shut down, but bandwidth is merely throttled.

The benefits of restricting accessibility are manifold. First, the restriction of previously accessible social media platforms means the collective organization of dissent and rebellion must revert back to slower forms of communication, which can lead to significant delays and inefficiencies for opposition movements. Online message systems have revolutionized the way in which resistance groups and insurgencies stay connected, and losing said access can deal a significant blow to groups intent on maintaining a cohesive and hierarchical opposition to the government. Reports from both the Syrian and Libyan battlefields even indicate that unexpected interruptions of Internet accessibility can stifle groups' military capabilities, by cutting off their access to important geographical services, such as Google Earth (Keating, 2013).

But even where opposition groups have developed the capacity to maintain cohesion and control in the absence of network access, the shutdown of connectivity allows government to further isolate groups from their core support network. In contentious contexts where opposition groups are resisting or even actively fighting the government, garnerning and maintaining support for the opposition can be a key strength of otherwise weak actors (Arreguin-Toft, 2001; Valentino, Huth and Balch-Lindsay, 2004). In modern conflicts opposition groups are increasingly relying on digital channels to reach both new potential supporters and fresh recuits. Material support no longer requires local interactions,

when financial transactions can be made through mobile phones. Individuals in distant locations can demonstrate their solidarity through the spreading of messages as well as the collection of financial support. When governments limit Internet accessibility in areas where opposition and resistance groups are located they thus not only hinder said groups' abilities to organize and fight, they also limit their access to moral and material support.

Lastly, restricting digital communication channels can significantly complicate the exchange of information that is critical of the government. Reducing the volume of local 'negative press' can make it increasingly hard for individuals to assess the extent to which fellow citizens are frustrated with the political status quo, and possibly willing to resist or fight to change it. As a consequence, citizens may revert to falsifying their preferences, by keeping their true opinion to themselves, as open opposition is deemed to risky (Kuran, 1997).

While this process may lead to a temporary increase in outward-facing obedience, the lack of local information on regime support and dissatisfaction may prove dangerous in the long run (Lorentzen, 2013). Where a government has opted for the use of Internet disruptions to avert further spread of unrest, it has therefore simultaneously limited its own access to crucial intelligence. I argue that governments limiting access to the Internet are likely to implement this form of control in conjunction with violent coercive strategies that are *indiscriminate in terms of whom they target.* Not only are anti-government groups barred from organizing online, state forces now also lack access to information about the disaffected citizens. In addition, loyal civilian supporters of the government are prohibited from sharing knowledge about developments on the ground with them via the Internet (Shapiro and Weidmann, 2015). In short, states sabotage their own access to information on the identity and location of the most 'dangerous' dissidents. The use of violence will inadvertently become increasingly indiscriminate. *I therefore expect that government restrictions on the free exchange of information are likely to be positively associated with a larger, untargeted coercive response tactic.*

Under what conditions are digital controls useful for regimes?

While ample research suggests that governments across the world are heavily investing in Internet controls (Deibert, 2003), their importance for informing states repressive strategies are likely to vary, both across regimes[2] and by local context within regimes. Here, I focus on local differences.

Digital controls are likely to be particularly important where other forms of more traditional control are proving to be less effective. For example, digital surveillance will prove to be more useful where state forces have fewer opportunities to tap into other networks to obtain critical information needed to target specific dissidents and opposition activists. Conversely, in areas that offer alternative means of obtaining such information states will be less reliant on digital forms of surveillance to achieve their goals. For example, in areas traditionally known to exhibit strong loyalties for the ruling regime (for example through ethnic, religious or political linkages) digital surveillance may play less of a role in acquiring information about 'enemies of the state' as government supporters may be more willing to freely share such information with state authorities. Digital disruptions that aim at limiting access to the Internet may even backfire in such areas, as those loyal to the government may feel they are being unnecessarily punished.

In contexts where the government is fighting armed internal opposition groups, citizens are more likely to feel safe in sharing such information where the government exhibits a strong local presence, such as when it controls the majority of the territory (Kalyvas, 2006). Digital surveillance is thus likely to be particularly useful for governments in areas that are not fully on their control. *I therefore expect that government provisions for the free exchange of information (enabling digital surveillance) will be positively associated with a targeted repressive campaign, in particular in areas not fully controlled by regime.*

[2]The importance of digital controls in states' repressive strategies may vary between regimes in terms of states' capacities to implement and make use of digital controls effectively, the level of Internet penetration within a given country, and the degree to which opposition or dissident groups rely on digital communication.

Digital controls in the Syrian Conflict

Surveillance and Internet restrictions have a long history in Syria, where the first nationwide monitoring system was commissioned by the Syrian Telecommunications Establishment (STE) in 1999 (Privacy International, 2016, 8). A few weeks before the first mass protests ensued across Syria in March 2011, the regime led by President Bashar Al-Assad lifted a large number of bans on social networking platforms, including Facebook and YouTube. Up to that point, the Assad regime had maintained the most regulated media and telecommunications landscape in the Middle East (OpenNet Initiative, 2009).

The Syrian regime's extensive use of surveillance technology following the unblocking of social media suggests that the government's intentions behind lifting the ban were to obtain information on the location, identity and extent of opposition activities within its own borders. Lifting the ban offered the regime a low-cost and effective way to expand surveillance and gain a clearer picture of state enemies (see e.g. MacKinnon, 2012). Over the course of the conflict, the regime has also implemented irregular nationwide shutdowns of the Internet, but more importantly, it has strategically limited accessibility in different parts of the country (Freedom House, 2015). Telecommunications in Syria remain highly centralized, allowing the government to maintain in full control of the network. Shutting down the Internet as systematically as has been observed in Syria suggests that the shutdowns are implemented through technical configurations, and not through physical failures or cut cables (Perlroth, 2013).

Given the central role social media has played for all actors involved in the conflict, the Syrian government's use of surveillance techniques and Internet controls comes as no surprise. Researchers have documented the use of blanket communication monitoring technology (Privacy International, 2016), imported surveillance and censorship software (Chaabane et al., 2014), targeted malware attacks against opposition groups (Galperin, Marquis-Boire and Scott-Railton, 2013), and the employment of their own 'Syrian Electronic Army' (Al-Rawi, 2014).

In a 2016 report, Privacy International summarized Syrian Internet control accordingly (Privacy International, 2016, 8):

> The Government maintains tight control of telecoms services through the telecom regulator and owner of the nation's telecommunications infrastructure, Syrian Telecommunications Establishment (STE). The use of censorship technologies to filter political, social, and religious websites, and to conduct surveillance on citizens is widespread. Targeted cyberattacks including general phishing, more targeted 'spear-phishing', the use of malware and 'Trojan horse' viruses against individuals and organizations; and distributed denial of service (DDoS) attacks against websites are widespread. Journalists and activists have been identified using these tactics and subsequently arrested.

Researchers have repeatedly highlighted the extensive use of surveillance to identify activists and defectors on social media. For example, phishing attacks, where users are coaxed into submitting their usernames and passwords on fake webpages, are used to infiltrate individuals' social network accounts and glean identity and location information of other activists. When individuals are arrested, they are then usually required to share the passwords of their social media and email accounts (Hashem, 2015), allowing authorities to use these to gather more information. Anecdotal evidence suggests that opposition members and activists exposed to malware have thereafter been arrested, and have had interrogators mention interception of digital information them (Marczak et al., 2014, 7-8).

The Syrian Conflict therefore presents a suitable case to empirically test for the interplay between government-implemented Internet controls and the use of violence repression. The Syrian government has a long history of mass surveillance of its population, and due to monopolization of the telecommunications sector remains in full control of the national Internet infrastructure. It is therefore reasonable to assume that where Internet accessibility is being limited, it is being limited intentionally, and where it is not being limited, this freedom of access is equally intentional. It is also reasonable to assume that where Internet accessibility is available, surveillance technology is being employed.

Data

To investigate the relationship between Internet accessibility and the type of repressive strategy, I analyze the Syrian government's use of targeted and untargeted violence between June 2013 and April 2015, in two-week intervals. For each of the 14 Syrian governorates and every two-week time period, I establish the number of targeted killings (y_{jt}), and the number of untargeted killings (z_{jt}), which together form the overall number of killings per observation ($N_{jt} = y_{it} + z_{it}$).

A new measure for regime violence

The analysis relies on combined information about lethal violence in Syria that was collected by four different data documentation groups: the Syrian Center for Statistics and Research (CSR-SY)[3], the Syrian Network for Human Rights (SNHR)[4], the Damascus Center for Human Rights Studies (DCHRS) Website[5], and the Violations Documentation Centre (VDC)[6]. Each group documents individual killings, including the victims' names, date of death, location, and a number of covariates, including the cause of death and the circumstances under which the death occurred. The detailed circumstantial information available for each victims allows the analysis to move beyond body counts towards a more fine-grained measure on the nature of violence used by the Syrian government at a specific time and location.

To compile the full database, I pooled all records by the four sources into one dataset, and performed semi-supervised record-linkage techniques in order to account for killings that were documented by more than one source.[7] Each record is compared to every other record in order to identify records that refer to the same victim. Some victims were found in two, or three, or even in all four original data sources. Others were only documented by one group.

[3] http://csr-sy.org/
[4] http://www.syrianhr.org/
[5] http://www.dchrs.org/english/news.php?aboutus
[6] http://www.vdc-sy.org/
[7] See appendix for detailed information on the record-linkage procedure.

For each unique killing, the documentation provided by the different sources on event circumstances is clustered so as to obtain as much information per record as possible.[8] To categorize each record as a specific type of killing (either targeted or untargeted), I make use of supervised text classification. Based on a training set of 2347 records which I classified by hand, I train the model to predict the type of killing for the remaining records. A third category is classified which includes all victims killed by non-government forces, which I drop from the analysis.[9]

The operational definition for targeted and untargeted violence used here builds on work by Kalyvas (2006), Steele (2009), and Wood (2010). In this context, state violence is defined as targeted if the victim was killed either due to individual or collective characteristics. Since it is not possible to measure the government's intent directly, I rely on documented information regarding the circumstances of violence to infer the probable intent. All incidences where the victim was not selected on the basis of individual or collective characteristics, are assumed to be the result of untargeted violence. I use supervised machine-learning to classify over 65,000 aggregated reports on individual killings that were committed by the Syrian regime (and pro-government forces) between June 2013 and April 2015.

In the hand-coded training set, records are classified as **targeted** killings if the circumstances described in the aggregated report 1) indicate that the victim was selected based on his/her specific characteristics *(e.g. 'killed because he refused to[...]', 'dissent')* and/or 2) indicate that the method of killing was of a selective nature *(e.g. executed by sniper, hanging, beheading, set afire)*, and/or 3) the method of killing was accompanied by other violations of a selective nature *(e.g. arrest, detention, prison, 'found with hands/legs tied')*. The majority of targeted killings are classified based on method of killing, or accompanying violations (e.g. torture) that indicate targeting.

Records are classified as **untargeted** killings if the circumstances described in the aggregated report 1) indicate that the victim was not selected based on his/her specific characteristics *(e.g. 'stepped on a landmine')*, and/or indicate that the method of killing

[8] See appendix for details and examples.

[9] Since all of the documentation groups focus on violence perpetrated by regime forces, the number of records collected on killings in this third category is too small to provide a representative sample of non-regime perpetrated killings.

was not selective *(e.g. explosion, bombing, shelling, mortar, chemical, toxic cases)*, and/or 3) the method of killing was not accompanied by other targeted violations.[10]

The classification presented here uses the gradient booster *xgboost* (Chen et al., 2017) to classify the records according to these categories. A variety of different algorithms were tested, including support vector machine-learning and random forest models, however, the results based on the extreme gradient booster provided the highest overall algorithm performance. Performance statistics as well as the n-grams with the highest feature importance for each of the categories are reported in the appendix. Table A10 shows that the most important features for the classification model reflect the conceptual distinctions very well.

Of the 65,274 records, 2,380 of the recorded killings were perpetrated by other conflict actors and thus excluded from the analysis. The overwhelming majority of the records collected by the four human rights groups indicate untargeted violence, and more than 10,000 are classified as targeted instances of state repression.

Dealing with underreporting

Variations in reporting can be a serious problem in the analysis of event count data (Weidmann, 2016), in particular when attempting to compare patterns of categories of violence that occurred under different circumstances. Simple event counts are likely to be unrepresentative of actual patterns of violence in the present analysis. The likelihood that targeted and untargeted violent events are reported with a different probability is high. Furthermore, the main variable of interest - variations in Internet accessibility - may influence the ability to report, which by consequence would lead to reports of violence affecting to the level of information accessibility.

Through the de-duplication process all records that describe the same killing are collapsed, removing duplicate reports of the same incidence. Because the database merges 4 data sources, the overlaps (or intersections) between them can be used to estimate 4-system multiple recapture models that can predict the number of unreported regime killings (Lum,

[10]Note that the coding of targeted and untargeted killings is highly conflict and actor specific. For example, armed actors, such as the provisional IRA did in Northern Ireland (Heger, 2015), may use small-scale bombings to target their enemies. In the Syrian conflict, the use of barrel bombs and indiscriminate bombardment by the government as a means of indiscriminately killing civilians has been extensively documented (Pinheiro, 2015).

Price and Banks, 2013; Hendrix and Salehyan, 2015). The estimation of unreported regime fatalities helps account for possible underreporting in the datasources that would otherwise bias the results of the analysis. I opt for a set of multiple recapture models developed by Madigan and York (1997), which are designed to deal with dependency between different sources, as it occurs when different data collection efforts occasionally work together or have the same primary source. Details on the estimation prodecure can be found in the appendix.

Internet accessibility

To measure regional network accessibility in Syria, I make use of survey data collected by the Syria Digital Security Monitor (SDSM), a project funded by the SecDev Foundation.[11] Since June 2013, SDSM has surveyed all Syrian districts every two weeks[12] in order to establish the degree of digital accessibility across the country. The survey asks respondents to separately rate their ability to use the Internet (distinguishing between DSL, 2G, and 3G) as well as mobile phones, on a four-point scale, where 1 = general availability, 2 = available often, 3 = intermittent availability, and 4 = no availability. To ensure comparability, SDSM attempts to survey the same set of respondents in every wave, but also makes use of social media sources.[13] I test the effect of connectivity using two measures of wireless Internet connectivity (2G and 3G networks), and an additional measure for mobile phone network access. To obtain a standardised unit of analysis, the accessibility measures are aggregated to an average continuous measure of accessibility at the governorate level, measured in two-week intervals. To ease interpretation, the scale is reversed, so that lower values indicate lower levels of accessibility, and higher values indicate higher levels of accessibility.

Figure 1 plots the level of network accessibility (Mobile Phones, 3G and 2G) by governorate for the time period of this study, 01 June 2013 - 30 April 2015. Where the lines spike, regular or full Internet access is available. Governorates are shaded in red if they, on average where predominately controlled by the government (>80% government control),

[11] https://secdev-foundation.org/
[12] For a select few months, only one survey is available, not two.
[13] Personal communication with SecDev Foundation staff.

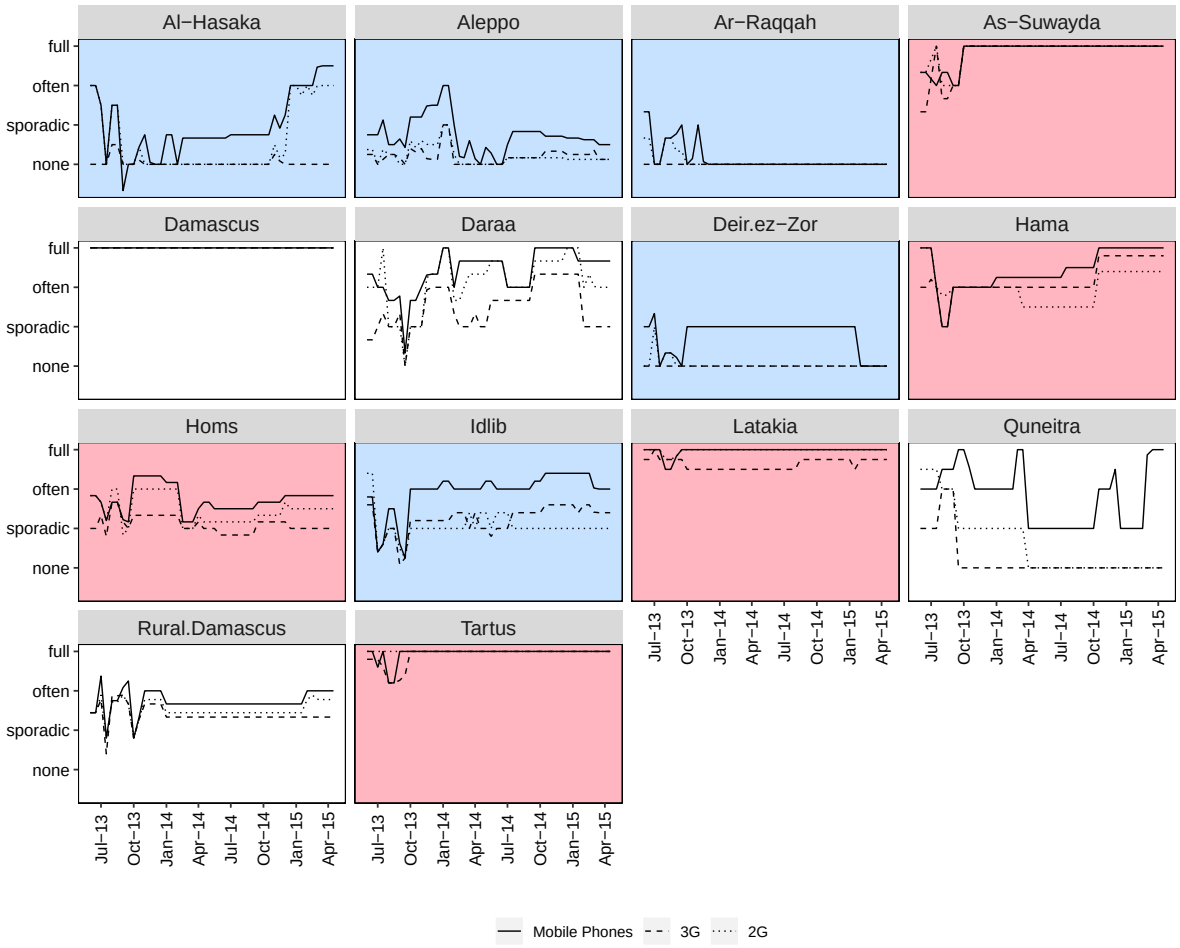


Figure 1. Network (mobile phones, 3G, and 2G) accessibility by Syrian governorate, June 2013 - April 2015.

and shaded in light blue they were, on average, predominately under the control of one of the other conflict actors (<20%). Some areas, such as Tartus (highly government controlled) and Damascus (contested) have had relatively uninterrupted internet access for the majority of the time under investigation. The Northern governorate of Ar-Raqqah (an IS stronghold throughout the period under investigation) is the only one to have been almost entirely cut off from both Internet and mobile phone access during the period under investigation. Many regions, however, have been subjected to high levels of fluctuation, including Hama, Homs, Idlib, Daraa, Aleppo, and the region surrounding the capital of Damascus (known as Rif Dimashq or Rural Damascus). While these regions have been at the center of some of the worst fighting between regime and opposition forces, the average level of control varies between them.

It is important to note that in all of these regions, accessibility is not continuously decreasing, a pattern we might expect to see if Internet access were tied to technical failures stemming from irreparable damage by destruction of infrastructure. Instead we see that access is frequently lost for short periods of time, and then increases again, only to decrease in the following month.

Confounders

Armed group presence. I rely on data collected by the Syria Conflict Mapping Project (SCMP) that is part of the Carter Center to construct an indicator of individual armed group presence and territorial control.[14] The SCMP collects the to date most accurate and detailed open source information on conflict events occurring across the country, including information on changing relationships between the main conflict actors. The project tracks more than 5000 local communities and determines which conflict party is in control. While the SCMP tracks thousands of local opposition groups, for the purpose of this study I follow their broad categorization of four main conflict lines: Opposition forces, Islamic State forces, Government forces, and Kurdish forces.[15]

I create a number of aggregate measures from the community-level control data that reflect armed group presence, control, and temporal changes in control at the governorate level to match the information on regime violence and Internet accessibility.

The main measure of control is a categorical variable which takes on the name of the group that has more than 60% of all communities in a governorate under its control. When and where none of the groups holds more than 60% (such as in Aleppo in January and July 2014), the variable is coded as *contested control.*[16] In order to measure the government's local presence more precisely, I also include the actual *percentage of control* for the government. To account for the changing role of Internet controls in different local contexts I interact both measures of armed group presence with levels of Internet accessibility.

[14]See https://www.cartercenter.org/syria-conflict-map/.

[15]See appendix for further details.

[16]I specify alternative models where I alter the 60% threshold to 70% , and find consistent results. See Table A6

Figure 2 shows the average proportion of targeted killings, depending on territorial control. Unsurprisingly, the proportion is highest in areas under government control. In area controlled by Kurdish forces, opposition forces, and areas where control is contested the proportion is significantly lower, yet still makes up a 14-15% of all killings. The proportion is lowest in areas controlled by the Islamic State.

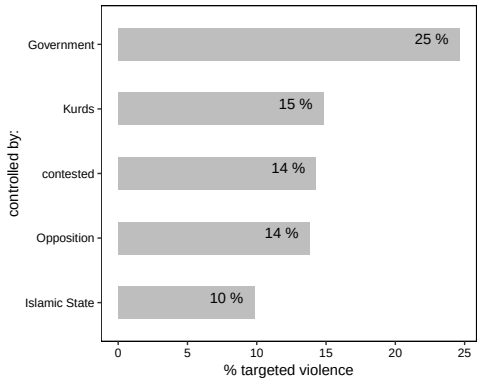


Figure 2. Percentage of violence that is targeted, by type of control.

The type of repression used by the government might be dependent on whether the government is losing or winning territory. A categorical variable based on the *percentages of control* measures whether the government gained or lost territory, or whether it remained constant (*govt gains/ govt losses/ constant*). For example, in January 2015 the government had lost territory in Aleppo, but gained ground in the North-Eastern Al-Hasaka.

Whether the government is predominately using targeted or untargeted repression at a given time in a given area is likely to also be dependent on their overall conflict engagement. To account for conflict intensity, I include the overall logged *number of killings* perpetrated by the government in the empirical model.

Politically relevant ethnic groups have made up an important part of the ongoing Syrian conflict. In addition to the predominant Sunni Muslims, the Alawi, Druze, Kurdish and Christian Syrians form politically ethnic groups. To measure ethnic group presence, I make use of the GeoEPR Dataset (Wucherpfennig et al., 2011) which codes the geographic location and time period of *politically relevant groups* for the entire world, starting in 1946. As the Assad regime belongs to, and has historically predominantly recruited its

inner circle from the Syrian Alawite community, I interact Alawi presence with Internet accessibility to account for other forms of control that may be at play in traditional government strongholds. To account for socio-demographic factors I include *population size* (logged), as well as levels of *unemployment* as a proxy of regional economic strength, which may influence both the government's willingness to restrict Internet access, as well as their choice of violence.[17] To account for unobserved temporal conflict dynamics I include temporal fixed-effects.

Results

The government's repressive tactic is operationalized as consisting of two components, namely the perpetration of targeted and untargeted killings. Comparing the number of targeted and untargeted killings to each other allows us to account for differences in the nature of violence across both time and locations. I therefore analyze both manifestations of violence within the same empirical model. For every two-week period t and governorate j, I model the number of targeted killings (y_{jt}) as compared to the total number of killings per observation (N_{jt}), which is the sum of targeted (y_{it}) and untargeted killings (z_{it}). I fit a generalized linear model, where:

$$y_{jt} \sim Bin(\pi_{jt}, N_{jt}) \tag{1}$$

and

$$\pi_{jt} = logit^{-1}(\beta * internet_{jt} + X_{jt}\gamma) \tag{2}$$

.

The dependent variable is the number of targeted killings y_{jt}, modeled as the proportion of the total number of killings N_{jt}.[18] The probability (π_{jt}) of an individual killing being either

[17]The data are downloaded from the Syrian Central Bureau of Statistics 2011 year book at: http://www.cbssyr.sy/yearbook/2011/Abstract_2011.rar

[18]The binomial regression model weighs observations by overall number of killings to account for uncertainty. For example, an observation where 300 of overall 1000 killings were targeted will be weighed more heavily than an observation where 3 of overall 10 killings were targeted, even though they both have the same percentage of targeted killings.

targeted or not is dependent on the level of internet accessibility $internet_{jt}$, parameter β, a number of control variables X_{jt} and a vector of parameters γ. X_{jt} includes the regression constant, as well as the variables previously discussed. All models are calculated with governorate-level clustered standard errors.[19]

Table I presents a number of regression models investigating the relationship between Internet accessibility (measured as third generation (3G) of wireless mobile Internet) and the proportion of targeted government repression.[20] The first model includes the basic set of explanatory variables, whereas the second model replicates the first with time fixed-effects. The AIC and BIC show that accounting for unobserved temporal dynamics considerably improves the model fit. The third model includes a measure for conflict intensity (log number of state-perpetrated killings), and the fourth model additionally accounts for territorial wins or losses on the side of the government.

[19]Section A.1 of the appendix replicates these results using negative binomial count models to investigate the relationship between Internet accessibility and the *number* of targeted killings, and the *number* of untargeted killings.

[20]Tables A3, A4, and A5 present results for alternative Internet access measures.

	I	II	III	IV	V	VI	VII
Intercept	−2.287***	−2.335***	−1.176**	−0.555	−0.344	−2.355	−5.002***
	(0.225)	(0.269)	(0.395)	(0.567)	(0.349)	(1.285)	(1.329)
Internet access (3G)	0.208*	0.229*	0.211*	0.208*	0.340**	0.367**	1.051***
	(0.097)	(0.091)	(0.085)	(0.086)	(0.114)	(0.117)	(0.140)
% Govt control							0.020***
							(0.004)
Internet (3G) * % Govt control							−0.015***
							(0.002)
Govt control	0.662	0.706*	1.003***	1.023***	0.325	0.882**	0.645*
	(0.348)	(0.282)	(0.301)	(0.307)	(0.360)	(0.324)	(0.264)
IS control	−0.241	−0.345	−0.671**	−0.644**	−1.152***	−0.804***	−0.820***
	(0.259)	(0.253)	(0.246)	(0.246)	(0.236)	(0.243)	(0.242)
Kurd control	0.311	−0.765	−0.649	−0.688	−0.455	0.340	−0.353
	(0.931)	(1.307)	(1.220)	(1.251)	(1.171)	(1.219)	(0.474)
Opp control	1.008**	1.071**	0.720*	0.759*	−0.527	−0.274	−0.211
	(0.340)	(0.364)	(0.337)	(0.352)	(0.299)	(0.374)	(0.175)
Internet (3G) * Govt control	−0.129	−0.161	−0.280*	−0.281*	−0.181	−0.387**	
	(0.135)	(0.115)	(0.122)	(0.124)	(0.141)	(0.124)	
Internet (3G) * Kurd control	−0.144	0.755	0.243	0.272	−0.146	−0.419	
	(0.735)	(1.023)	(0.953)	(0.973)	(0.915)	(0.887)	
Internet (3G) * Opp. control	−0.568***	−0.688***	−0.549**	−0.571**	0.237	0.287	
	(0.172)	(0.195)	(0.177)	(0.185)	(0.155)	(0.199)	
# Killings (log)			−0.204***	−0.206***	−0.317***	−0.381***	−0.551***
			(0.055)	(0.056)	(0.054)	(0.075)	(0.079)
Govt gains				0.427			
				(0.396)			
Govt losses				−0.156			
				(0.439)			
Alawi					1.145*	−1.254***	−0.855***
					(0.582)	(0.200)	(0.209)
Internet (3G) * Alawi					−0.875***		
					(0.182)		
Druze					−0.535**	−0.242	0.221
					(0.207)	(0.215)	(0.229)
Kurd					−0.407	−0.567*	−0.761**
					(0.226)	(0.273)	(0.248)
Christian					0.102	0.336**	0.408***
					(0.127)	(0.126)	(0.122)
Pop (log)						0.315	0.640***
						(0.180)	(0.182)
Unempl. (%)						−0.018	−0.005
						(0.013)	(0.013)
Temporal FEs		✓	✓	✓	✓	✓	✓
AIC	11708.555	9752.932	9569.229	9370.782	7700.895	7839.827	7310.605
BIC	11748.764	9994.187	9814.952	9619.742	7968.957	8112.357	7578.667
Log Likelihood	-5845.277	-4822.466	-4729.615	-4629.391	-3790.447	-3858.914	-3595.303
Deviance	9401.927	7356.304	7170.601	7025.006	5292.267	5429.200	4901.978
Num. obs.	640	640	640	626	640	640	640

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Contested control. Governorate-clustered SEs.

Table I. Internet accessibility (3G) and proportion of targeted killings (Generalized linear regression, binomial with logit link).

Across all four specifications, Internet accessibility is positively and significantly correlated with an increase in the proportion of targeted state violence, offering support to the relationship proposed in this paper. All models account for territorial control, where contested control is the reference category. The results show that across all models, areas with contested control display a positive and significant relationship between increased

Internet access and targeted killings. Where the government (nor any other group) has the upper hand, it is likely to use Internet access as a means to obtain intelligence that in turn supports targeted violence.

When controlling for unobserved time-specific effects, government control of a territory is a significant predictor of an increasingly targeted repressive campaign, when compared to areas of contested control. This confirms established theoretical and empirical findings on the relationship between territorial control and the nature of violence (see Kalyvas, 2006), which predict that in zones where armed actors control the territory, they will also be more likely to use a targeted repressive tactic. The results here thus also function as a validation of our repression measure. When controlling for conflict intensity and control, neither wins nor losses in government control are significantly associated with changes in targeted repression. Across the first four models, opposition-controlled areas are also associated with a more targeted campaign of violence than areas where control is unclear. And in areas controlled by the Islamic State, the results suggest that the state's repressive campaign is likely to be more indiscriminate. Conflict intensity is consistently negatively and significantly associated with lower proportions of targeted violence, suggesting that larger repressive campaigns tend to be more indiscriminate in nature.

Model 5 shows that the association between Internet access and state violence is mediated by the presence of Alawi citizens, who are traditionally known for their loyalty towards the Assad regime. While Internet access remains significant in this model, the interaction term between accessibility and Alawi presence is both negative and significant. Figure 3 simulates the expected proportion of targeted killings (based on Model 5, with 95% confidence intervals), given no or full Internet accessibility, in both Alawi and non-Alawi regions, using governorate-clustered standard errors. In non-Alawi regions, all else equal, the proportion of targeted killings perpetrated by the government is significantly and substantially higher when the Internet is fully accessible than when the Internet is shut down. In areas that are traditionally known to be inhabited by large amounts of regime supporters Internet accessibility, if anything, indicates a negative, relationship between access and targeted violence. The results offer support for the empirical expectations: Internet control, through the provision or limiting of accessibility, will be a useful tool for

governments to enhance their repressive capabilities, in particular when and where they cannot rely on other forms of more traditional control mechanisms.

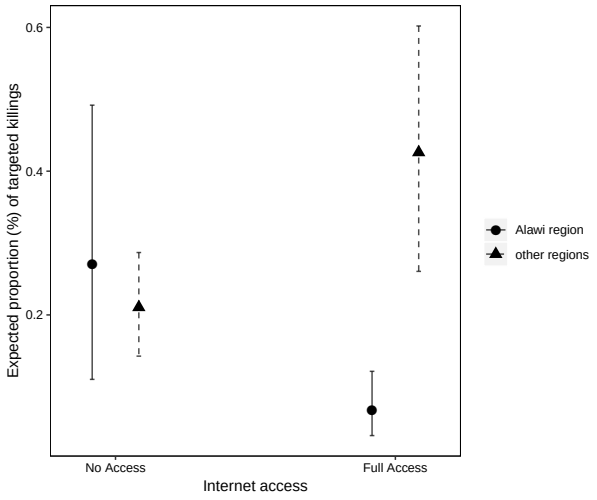


Figure 3. Expected proportion of targeted killings, given Internet accessibility and whether a region is inhabited by the Alawi minority.

Model 6 further includes measures for population size and unemployment, while model 7 accounts for a more nuanced relationship between Internet access, control, and targeted repression, by including the percentage of government control in a given region, as well as the interaction between government control and Internet accessibility. Internet accessibility is consistently associated with higher proportions of targeted violence. Other variables of interest exhibit fluctuating results. More populous regions seem to be associated with higher proportions of targeted violence, but the results are only significant when the more fine-grained measure of government control is included in model 7. Regions with Druze presence are also associated with lower proportions of targeted repression, but when controlling for population size and unemployment the results don't hold. Regions with Christian presence are significantly associated with higher proportions of targeted repression through the regime, and regions with Kurdish presence with lower proportions, when controlling for population size and unemployment.

Figure 4 simulates the expected proportion of targeted killings given different levels of Internet accessibility, and different degrees of government control. The left panel shows the relationship between Internet accessibility and targeted repression, where all other variables are held constant, and the government is in control of only 20% of the territory.

An example of this would be Idlib governorate in northwestern Syria in early 2014. The expected proportion of targeted killings in areas where the government has little control and where there is no Internet access is around 15%, which is corroborated the numbers presented in Figure 2. However, holding government control constant, the left panel shows that with increasing Internet accessibility, the proportion of targeted killings increases significantly and substantially. The middle panel shows the same relationship between Internet access and targeted repression for a scenario where the government controls 40% of the territory. The proportion of targeted repression starts out at a similar level, but the increase, while still substantial, is not as pronounced as in the previous panel. The right panel simulates areas where the government controls the majority of the territory. The proportion of targeted violence starts out at a significantly higher level, indicating that the government uses more targeted violence in areas it controls, regardless of Internet accessibility. But here, increasing Internet accessibility is not associated with a significant increase in targeted killings, indicating that the regime is likely relying on more traditional forms of intelligence gathering in areas under their own control.

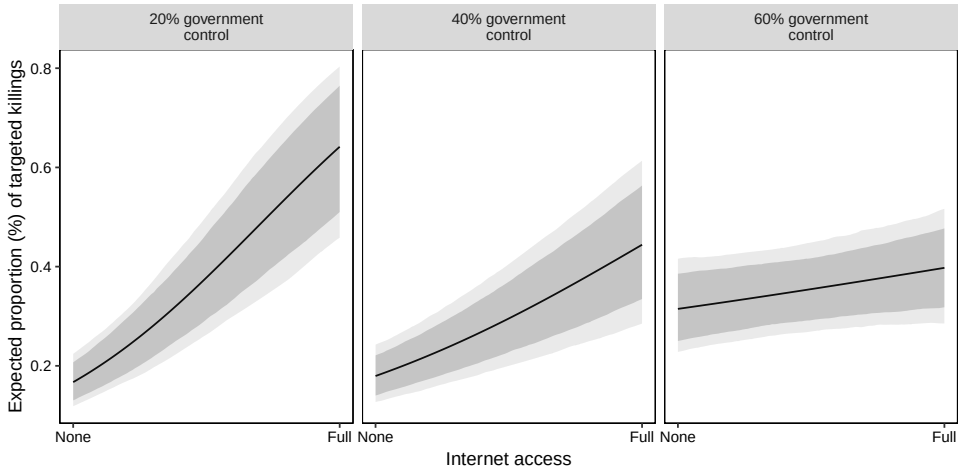


Figure 4. Expected proportion (83% and 95% confidence intervals) of targeted killings, given Internet accessibility and different levels of government control.

Figure 4 shows that the relationship between Internet accessibility and state repression is clearly mediated by levels of local territorial control. Internet control loses its importance with increasing government strength at the local level. Here, other forms of more traditional control allow the government to calibrate its repressive response. In contrast, Internet accessibility is significantly associated with a substantive increase in targeted

repression when and where the government has less local power. Here, Internet controls constitute a crucial tool in the regime's repressive strategy.

Conclusion

Much has been written about how digital technology is changing the way non-state groups come together to mobilize against repressive governments, some studies pointing to the ways in which increasingly networked populations will experience more (Pierskalla and Hollenbach, 2013) or less (Shapiro and Weidmann, 2015) non-state violence. Yet little is currently known about how governments use their ability to control the Internet to inform their own use of coercion. In this paper I argue that governments strategically manipulate Internet control - the provision or limiting of Internet access - as part of their repressive toolkit.

The analysis presented in this paper offers a number of interesting findings. Across a range of model specifications it shows that higher levels of Internet accessibility granted by the government are significantly and substantially associated with a more targeted strategy of regime violence. In contrast, where Internet access is limited or shut down, the Syrian government employs a significantly more indiscriminate campaign of violence. However, this relationship is mediated by local conditions that determine whether the regime is able to rely on more traditional forms of intelligence, or whether digital surveillance will enhance their ability to target those deemed threatening to their political survival. The results show that Internet controls become increasingly important with decreasing levels of government control. In contrast, areas inhabited by the Alawi minority, traditionally known to support the Assad regime, Internet accessibility is not associated with higher levels of targeted violence. In such areas the government is more likely to rely on conventional forms of obtaining information. Similar dynamics are observable in regions and at times when the government controls most of the territory.

The analysis presented here studies a large-scale civil conflict involving a highly repressive government as well as numerous violent armed non-state actors. It represents a more extreme case in which a government makes use of coercive measures against challenges to

its political stability. The repressive choices discussed in this paper, however, are likely to be relevant in other contexts where governments are prepared to use repressive tools against a real or perceived threat. While the scale at which states will use violence will differ, mass uprisings or even smaller-scale protests perceived to be of particular danger to the government's stability may trigger similar choices. Evidence suggests that the Bahraini government has used an arsenal of hacking tools to target activists prior to arresting them. In Ethiopia, the government shut down Internet access and reportedly killed almost a hundred protesters in the summer of 2016. In Sudan, Internet access was cut in September 2013 amidst a violent crackdown on anti-government protesters.

While repressive governments are adapting their tactics to the new digital reality of conflicts, previous research on surveillance suggests that these new methods will also stimulate learning on the side of the opposition (Sullivan and Davenport, 2018). Indeed, activists across Syria have, as the conflict progresses become increasingly savvy in circumventing digital controls, for example by making use of encrypted software, switching to conventional walkie-talkies when planning military offensives, and listening in on the regime's military communications (Hanna, 2015). The Syrian case underlines how opposition reliance on the Internet can clearly be a double-edged sword. At the individual level, the acquisition of sophisticated knowledge of ways to securely communicate, work, live, and travel without leaving a digital footprint may well become a matter of survival for anyone intending to challenge repressive government. At the international level, legal and normative pressure to regulate the export of dual-use technology intended to be used against regular citizens and political opponents will be of utmost importance to tackle this issue (Wagner et al., 2015).

The findings bear important implications for future dynamics of violent conflict. The evidence presented here suggests that Internet controls could provide tech-savvy governments with a new tactical advantage in civil conflicts, whereby they may now be able to access information on zones of conflict that were previously hard to access with more conventional intelligence tools. Even before unrest becomes visible, citizens showing signs of opposing viewpoints are now liable to be placed under close surveillance, long before their political preferences become publicly known. This, in turn, is likely to influence the characteristics of regime stability, opposition tactics, the propensity for full-fledged

conflict, and the nature of conflict termination in ways that are to date entirely under-researched. Both research and policy will have to rethink the role of Internet control in state repression.

References

Aday, Sean, Henry Farrell and Marc Lynch. 2010. "Blogs and Bullets: New media in contentious politics." *United States Institute of Peace, Peaceworks* 65.
URL: *https://www.usip.org/publications/2010/09/blogs-and-bullets-new-media-contentious-politics*

Al-Rawi, Ahmed K. 2014. "Cyber warriors in the middle east: The case of the syrian electronic army." *Public Relations Review* 40(3):420–428.

Arreguin-Toft, Ivan. 2001. "How the weak win wars: A theory of asymmetric conflict." *International Security* 26(1):93–128.

Chaabane, Abdelberi, Terence Chen, Mathieu Cunche, Emiliano De Cristofaro, Arik Friedman and Mohamed Ali Kaafar. 2014. Censorship in the wild: Analyzing Internet filtering in Syria. In *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM pp. 285–298.

Chen, Tianqi, Tong He, Michael Benesty, Vadim Khotilovich and Yuan Tang. 2017. *xgboost: Extreme Gradient Boosting*. R package version 0.6-4.
URL: *https://CRAN.R-project.org/package=xgboost*

Deibert, Ronald J. 2003. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium* 32(3):501–530.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain and Miklos Haraszti. 2010. *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Earl, Jennifer and Katrina Kimport. 2011. *Digitally enabled social change: Activism in the internet age*. Cambridge, MA: MIT Press.

Freedom House. 2015. "Syria." *Freedom on the Net 2015* . (accessed 2018-07-01).
URL: *https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Syria.pdf*

Galperin, Eva, Morgan Marquis-Boire and John Scott-Railton. 2013. Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns. Technical report Citizen Lab and Electronic Frontier Foundation. (accessed 2018-07-01).
URL: *https://www.eff.org/document/quantum-surveillance-familiar-actors-and-possible-false-flags-syrian-malware-campaigns*

Gohdes, Anita R. 2015. "Pulling the plug: Network disruptions and violence in civil conflict." *Journal of Peace Research* 52(3):352–67.

Gunitsky, Seva. 2015. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13:42–54.

Hanna, Asaad. 2015. "How Syrian opposition bypasses Assad's communication blocks." *Al-Monitor* . (accessed 2019-01-15).
URL: *www.al-monitor.com/pulse/originals/2015/12/syria-opposition-means-of-communication-regime.html*

Hashem, Mohamed. 2015. "Q&A: In Syria the 'internet has become a weapon' of war." *Al-Jazeera* . (accessed 2017-10-01).
URL: *http://www.aljazeera.com/indepth/features/2015/06/qa-syria-internet-weapon-war-150619215453906.html*

Hassanpour, Navid. 2014. "Media Disruption and Revolutionary Unrest: Evidence From Mubarak's Quasi-Experiment." *Political Communication* 31(1):1–24.
URL: *https://doi.org/10.1080/10584609.2012.737439*

Heger, Lindsay L. 2015. "Votes and violence: Pursuing terrorism while navigating politics." *Journal of Peace Research* 52(1):32–45.
URL: *https://doi.org/10.1177/0022343314552984*

Hendrix, Cullen S. and Idean Salehyan. 2015. "No News Is Good News: Mark and Recapture for Event Data When Reporting Probabilities Are Less Than One." *International Interactions* 41(2):392–406.

Hounshell, Blake. 2011. "The Revolution Will Be Tweeted." *Foreign Policy* 20 June.
URL: *http://www.foreignpolicy.com/articles/2011/06/20/the_revolution_will_be_tweeted*

Kalathil, Shanthi and Taylor C. Boas. 2003. *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Washington: Carnegie Endowment for International Peace.

Kalyvas, Stathis. 2006. *The Logic of Violence in Civil War*. New York: Cambridge Univeristy Press.

Keating, Joshua. 2013. "Firing Mortars? There's an App for That." *Slate* 18 September. (accessed 2018-07-01).
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.

King, Gary, Jennifer Pan and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111(3):484–501.

Kuran, Timur. 1997. *Private truths, public lies: The social consequences of preference falsification*. Cambridge, MA: Harvard University Press.

Little, Andrew T. 2016. "Communication Technology and Protest." *Journal of Politics* 78(1):152–166.

Lorentzen, Peter L. 2013. "Regularizing rioting: permitting public protest in an authoritarian regime." *Quarterly Journal of Political Science* 8(2):127–158.

Lum, Kristian, Megan Emily Price and David Banks. 2013. "Applications of Multiple Systems Estimation in Human Rights Research." *The American Statistician* 67(4):191–200.

Lyon, David. 2009. *Surveillance studies: An Overview*. Cambridge, MA: Polity Press.

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

Madigan, David and Jeremy C. York. 1997. "Bayesian Methods for Estimation of the Size of a Closed Population." *Biometrika* 84(1):19–31.

Marczak, William R., John Scott-Railton, Morgan Marquis-Boire and Vern Paxson. 2014. When Governments Hack Opponents: A Look at Actors and Technology. In *Proceedings of the 23rd USENIX Security Symposium*. (accessed 2017-07-01).
URL: *https://www.usenix.org/node/184470*

Morozov, Evgeny. 2012. *The net delusion: The dark side of Internet freedom*. New York: Public Affairs.

OpenNet Initiative. 2009. "Internet Filtering in Syria." OpenNet Country Profile.
URL: *https://opennet.net/research/profiles/syria*

Perlroth, Nicole. 2013. "Syria, and Pro-Government Hackers, Are Back on the Internet.".
URL: *http://nyti.ms/L8zhO7*

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(2):207–224.

Pinheiro, Paulo Sérgio. 2015. "The use of barrel bombs and indiscriminate bombardment in Syria." *Independent International Commission of Inquiry on the Syrian Arab Republic* . (accessed 20 November 2018).
URL: *https://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/CoISyriaIndiscriminateB*

Privacy International. 2016. "Open Season: Building Syria's Surveillance State.". (accessed 2018-07-01).
URL: *https://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state*

Roberts, Margaret E. 2018. *Censored: Distraction and Diversion Inside Chinas Great Firewall*. Princeton: Princeton University Press.

Shadmehr, Mehdi and Dan Bernhardt. 2012. "A Theory of State Censorship." *APSA 2012 Annual Meeting Paper* .
URL: *https://ssrn.com/abstract=2105407*

Shapiro, Jacob N. and Nils B. Weidmann. 2015. "Is the Phone Mightier than the Sword? Cell Phones and Insurgent Violence in Iraq." *International Organization* 69(02), 247-274.

Steele, Abbey. 2009. "Seeking Safety: Avoiding Displacement and Choosing Destinations in Civil Wars." *Journal of Peace Research* 46(3):419–429.

Steinert-Threlkeld, Zachary C. 2017. "Spontaneous Collective Action: Peripheral Mobilization During the Arab Spring." *American Political Science Review* 111(2):379–403.

Sullivan, Christopher M and Christian Davenport. 2018. "Resistance is mobile: Dynamics of repression, challenger adaptation, and surveillance in US 'Red Squad' and black nationalist archives." *Journal of Peace Research* 55(2):175–189.
URL: *https://doi.org/10.1177/0022343317749273*

Tufekci, Zeynep. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press.

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

Van Belle, Douglas A. 1997. "Press Freedom and the Democratic Peace." *Journal of Peace Research* 34(4):405–414.

Wagner, Ben, Joanna Bronowicka, Cathleen Berger and Thomas Behrndt. 2015. "Surveillance and censorship: The impact of technologies on human rights." *European Parliament: PE 549.034* . (accessed 2018-03-01).
URL: *http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549*

Weidmann, Nils B. 2016. "A closer look at reporting bias in conflict event data." *American Journal of Political Science* 60(1):206–218.

Whitten-Woodring, Jenifer. 2009. "Watchdog or Lapdog? Media Freedom, Regime Type, and Government Respect for Human Rights." *International Studies Quarterly* 53(3):595–625.

Wood, Elisabeth J. 2010. Sexual Violence During War: Variation and Accountability. In *Collective Violence and International Criminal Justice*, ed. Alette Smeulers. Vol. 8 Antwerp: Intersentia chapter 13, pp. 297–324.

Wucherpfennig, Julian, Nils B. Weidmann, Luc Girardin, Lars-Erik Cederman and Andreas Wimmer. 2011. "Politically Relevant Ethnic Groups across Space and Time: Introducing the GeoEPR Dataset." *Conflict Management and Peace Science* 28(5):423–437.

Supporting Information for: 'Repression technology: Internet accessibility and state violence'

Overview

A Additional analyses: Internet accessibility and regime repression

The following sections present additional analyses on the relationship between Internet accessibility and regime repression.

A.1 Count model analyses: Absolute number of targeted and untargeted killings

Table A1 presents results for count models[21] investigating the relationship between Internet accessibility and the number of targeted killings (first, third, and fifth model) and the number of untargeted killings (second, fourth, and sixth model). The models replicate Models III, V, and VII in Table I, estimating negative binomial models with temporal fixed effects and governorate-clustered standard errors. Models III, V and VII were chosen because they include two different types of interactions between government control and Internet accessibility, as well as the interaction between Internet accessibility and traditional regime strongholds. Model III interacts categorical representations of control with Internet accessibility, thus accounting for specific dynamics depending on differing conflict actors. Model V includes an interaction term between Internet accessibility and Alawi presence. Model VII categorically accounts for different conflict actors maintaining territorial control, but interacts the percentage of government control with the level of Internet accessibility, thereby allowing for a more nuanced interaction between the degree of government control and Internet access.[22]

Table A1 offers a number of interesting insights into the relationship between Internet access and state violence, and to what extent this relationship is mediated by local dynamics and context. Across all models higher levels of Internet accessibility are positively and significantly associated with higher number of targeted killings. In contrast, the models where the dependent variable is the number of untargeted killings suggest that there is no straightforward, significant relationship between Internet accessibility and untargeted violence. Significance levels alone can be misleading and so it is instructive to simulate expected changes in the number of targeted and untargeted killings for specific quantities of interest. To do so, I simulate the expected number of each type of killing, given different levels of Interent access in areas of contested territorial control (where no conflict party holds more than 60% of the territory). Recall that we expect Internet accessibility to be particularly important in areas not traditionally loyal to the regime, or not currently under its control.

[21] All models are estimated in R, using the standard `glm.nb` function.

[22] Note that the models in Table A1 do not include the total number of killings as an independent variable as this measure adds up the number of targeted and untargeted killings per observation. Furthermore, the replication of Model V (models three and four) exclude other ethnic group presence, as the negative binomial model failed to converge with their inclusion.

	Targeted #	Untargeted #	Targeted #	Untargeted #	Targeted #	Untargeted #
Intercept	2.674***	5.251***	2.755***	5.261***	−6.824***	−2.007*
	(0.326)	(0.233)	(0.255)	(0.233)	(1.119)	(0.864)
Internet access (3G)	0.326***	0.031	0.310***	0.031	1.133***	0.202
	(0.083)	(0.085)	(0.079)	(0.085)	(0.130)	(0.118)
Govt control	2.694***	2.056***	2.081***	2.014***	0.914***	0.623*
	(0.299)	(0.251)	(0.275)	(0.254)	(0.239)	(0.242)
IS control	−1.838***	−1.634***	−1.816***	−1.637***	−0.845***	−0.489*
	(0.188)	(0.183)	(0.187)	(0.183)	(0.192)	(0.219)
Kurd control	−0.222	−0.362	−0.214	−0.384	0.663	0.917**
	(0.786)	(0.817)	(0.798)	(0.819)	(0.374)	(0.341)
Opp control	−0.598*	−1.746***	−1.100***	−1.726***	−0.220	−0.056
	(0.282)	(0.284)	(0.279)	(0.283)	(0.153)	(0.159)
Internet * Govt control	−1.010***	−0.849***	−0.708***	−0.832***		
	(0.116)	(0.099)	(0.107)	(0.102)		
Internet * Kurd control	−1.527*	−1.726*	−1.528*	−1.706*		
	(0.657)	(0.711)	(0.668)	(0.715)		
Internet * Opp. control	0.015	0.728***	0.442**	0.654***		
	(0.133)	(0.141)	(0.147)	(0.161)		
Alawi			2.055***	0.515	−0.040	1.032***
			(0.399)	(0.415)	(0.163)	(0.137)
Internet * Alawi			−1.134***	−0.148		
			(0.122)	(0.115)		
Druze					0.820***	1.042***
					(0.172)	(0.152)
Kurd					−1.422***	−0.994***
					(0.186)	(0.148)
Christian					0.483***	−0.095
					(0.110)	(0.101)
Pop (log)					1.245***	1.087***
					(0.127)	(0.096)
Unempl. (%)					−0.054***	−0.072***
					(0.012)	(0.010)
% Govt control					0.028***	0.004
					(0.004)	(0.004)
Internet * % Govt control					−0.021***	−0.008***
					(0.001)	(0.001)
Temporal FEs	✓	✓	✓	✓	✓	✓
AIC	4935.969	7036.539	4759.284	7039.223	4363.279	6717.189
BIC	5181.692	7282.263	5013.942	7293.882	4631.341	6985.251
Log Likelihood	-2412.984	-3463.270	-2322.642	-3462.612	-2121.640	-3298.595
Deviance	751.548	726.208	745.056	726.189	755.928	721.172
Num. obs.	644	644	644	644	644	644

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Contested control. Governorate-clustered SEs.

Table A1. Internet accessibility and level number of targeted and untargeted killings (Negative binomial regression).

The left panel in Figure A1 shows the expected numbers for targeted killings. Holding all other factors constant, in areas of contested control where the government has cut access to the Internet, the simulated expected level of targeted violence over a two week period amounts to approximately 20 fatalities. With increasing levels of accessibility, the expected number of targeted killings increases; where the Internet is fully available, the expected number rises to roughly 55 throughout a two-week period. Figure A2 plots the expected change in the number of killings in conteste areas, when changing accessibility from no Internet access to full access. The average expected change is an increase of 35 targeted killings (with a 95% confidence interval of 12 to 74 killings). The results presented in these figures support the theoretical expectation that all else equal, the level of targeted violence used by the regime is significantly and substantively associated with government provisions of Internet accessibility. In areas where the government can not

rely on traditional forms of control (or where it is not controlling the majority of the territory), full Internet accessibility is expected to lead to more than double the amount of targeted violence.

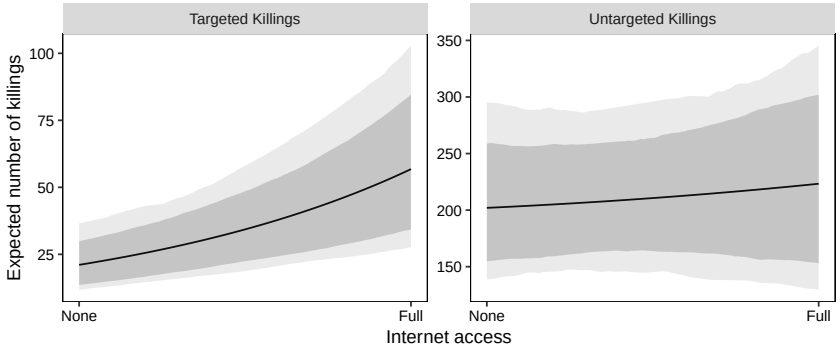


Figure A1. Expected number of targeted and untargeted killings, given levels of Internet accessibility, given contested control

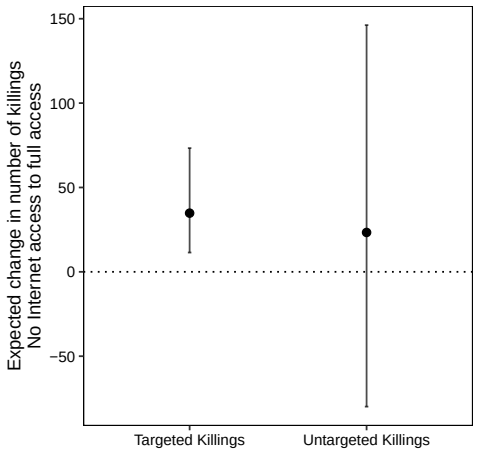


Figure A2. Expected change in the number of targeted and untargeted killings, given change from no to full Internet accessibility and given contested control.

Figures A1 and A2 also show the expected levels and changes in the number of untargeted killings in areas under contested control. The right panel in Figure A1 shows the overall expected level of untargeted violence in contested areas is substantially higher than the level of targeted violence. This is not surprising, as we know that indiscriminate attacks on civilians have been a central part of the Assad regime's campaign of violence, and that the percentage of targeted killings in contested areas is on average on 14% (see Figure 2). In contested areas with no Internet access, the expected number of untargeted killings is 200, all else equal. Where the Internet is fully accessible, the number is expected to be slightly higher (222 killings), but the large confidence intervals indicate that this change is highly uncertain. Supporting this, Figure A2 shows that the expected change in untargeted killings is close to zero, and the 95% confidence intervals includes both positive and negative values.

In conclusion, the analysis of absolute levels of targeted and untargeted violence offer further nuanced evidence for the relationship between Internet accessibility and state violence. Government provisions for an accessible Internet are positively and substantively associated with an increase in the level of targeted state violence perpetrated. This relationship holds for a variety of model specifications. In contrast, levels of untargeted violence are not directly associated with changing levels of Internet accessibility provided by the government. The results suggest that the relationship between the overall violent strategy of a government (as presented by the proportion of targeted vs. untargeted killings) and the government's decisions in controlling the Internet are principally driven by changes in the use of targeted killings. Freely accessible networks are clearly associated with more targeted violence. If targeted violence is perpetrated with the intention of eliminating specific individuals (or groups), then intelligence on the specific targets at hand will be crucial in supporting the governments strategic repressive goals. Levels of untargeted violence are likely to be dependent on a host of other factors that do not directly relate to whether intelligence is available via digital surveillance, or not.

A.2 Robustness checks: Varying measures of Internet accessibility and state violence

The following models investigate the proportion of targeted killings as a proportion of all killings in a given location at a given time. All models are estimated in R, using the standard `glm` function.

A.2.1 Time-lagged Internet access and state violence

	lagged 3G-I	lagged 3G-II	lagged 2G-I	lagged 2G-II	lagged Mob. Phone-I	lagged Mob. Phone-II
Intercept	−1.271	−3.728*	−1.758	−3.616**	−1.800	−2.776
	(1.329)	(1.473)	(1.289)	(1.404)	(1.403)	(1.563)
lag Internet/Mobile Phone access	0.229*	0.924***	0.295**	0.766***	0.179	0.500***
	(0.117)	(0.151)	(0.098)	(0.123)	(0.108)	(0.126)
Govt control	0.858**	0.806**	0.796*	0.845**	1.066*	0.836**
	(0.329)	(0.269)	(0.321)	(0.263)	(0.427)	(0.264)
IS control	−0.786**	−0.827***	1.431	−0.914***	0.162	−0.619*
	(0.240)	(0.243)	(0.817)	(0.248)	(0.618)	(0.260)
Kurd control	0.389	−0.339	1.171*	−1.419*	1.280	−0.522
	(1.235)	(0.474)	(0.562)	(0.599)	(0.716)	(0.515)
Opp control	−0.301	−0.236	−0.042	−0.198	−0.260	−0.081
	(0.351)	(0.176)	(0.301)	(0.169)	(0.462)	(0.165)
# Killings (log)	−0.380***	−0.567***	−0.323***	−0.510***	−0.339***	−0.473***
	(0.075)	(0.083)	(0.074)	(0.084)	(0.074)	(0.083)
Alawi	−1.146***	−0.763***	−1.204***	−0.792***	−1.052***	−0.782***
	(0.195)	(0.213)	(0.196)	(0.205)	(0.182)	(0.204)
Druze	−0.101	0.346	−0.282	0.198	0.021	0.404
	(0.197)	(0.226)	(0.212)	(0.228)	(0.178)	(0.227)
Kurd	−0.560*	−0.742**	−0.344	−0.546*	−0.431	−0.577*
	(0.259)	(0.250)	(0.243)	(0.236)	(0.245)	(0.247)
Christian	0.402**	0.476***	0.370***	0.397***	0.441***	0.442***
	(0.126)	(0.125)	(0.106)	(0.102)	(0.114)	(0.115)
Pop (log)	0.280	0.594**	0.253	0.530**	0.294	0.443*
	(0.180)	(0.194)	(0.170)	(0.183)	(0.176)	(0.195)
Unempl. (%)	−0.023	−0.011	−0.010	0.002	−0.018	−0.018
	(0.014)	(0.014)	(0.013)	(0.014)	(0.013)	(0.014)
lag Internet/Mobile Phone * Govt control	−0.310*		−0.266*		−0.268	
	(0.128)		(0.113)		(0.138)	
lag Internet/Mobile Phone * Kurd control	−0.437		−0.962**		−0.718*	
	(0.945)		(0.327)		(0.341)	
lag Internet/Mobile Phone * Opp. control	0.286		0.126		0.155	
	(0.179)		(0.113)		(0.156)	
lag Internet/Mobile Phone * IS control			−2.013**		−0.635	
			(0.686)		(0.409)	
% Govt control		0.018***		0.013**		0.014*
		(0.004)		(0.004)		(0.006)
Internet/Mobile Phone * % Govt control		−0.015***		−0.011***		−0.009***
		(0.002)		(0.002)		(0.002)
Temporal FEs	✓	✓	✓	✓	✓	✓
AIC	7755.862	7271.643	7701.330	7449.497	7758.115	7588.965
BIC	8022.605	7533.941	7972.518	7711.794	8029.304	7851.262
Log Likelihood	-3817.931	-3576.822	-3789.665	-3665.748	-3818.058	-3735.482
Deviance	5402.086	4919.868	5345.554	5097.721	5402.340	5237.189
Num. obs.	626	626	626	626	626	626

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Contested control. Governorate-clustered SEs.

Table A2. Lagged Internet/ Mobile Phone accessibility (at t-1) and proportion of targeted killings (Generalized linear regression, binomial with logit link). Models 1 and 2 account for 3G access, models 3 and 4 account for 2 G access, and models 5 and 6 account for Mobile Phone access.

A.2.2 2-G Internet access and state violence

	I	II	III	IV
Intercept	-2.318^{***}	-2.337^{***}	-0.956^{*}	-0.324
	(0.208)	(0.257)	(0.416)	(0.595)
Internet access (2G)	0.196^{**}	0.204^{**}	0.174^{**}	0.167^{**}
	(0.072)	(0.066)	(0.063)	(0.064)
Govt control	0.592	0.742^{*}	1.171^{***}	1.167^{***}
	(0.353)	(0.292)	(0.317)	(0.324)
IS control	2.657^{**}	2.705^{**}	2.258^{*}	1.790^{*}
	(0.956)	(0.946)	(0.882)	(0.859)
Kurd control	1.000^{*}	1.486^{**}	0.903	0.927
	(0.474)	(0.513)	(0.519)	(0.534)
Opp control	-0.134	0.080	-0.234	-0.223
	(0.421)	(0.374)	(0.353)	(0.371)
Internet (2G) * Govt control	-0.087	-0.147	-0.304^{**}	-0.296^{*}
	(0.121)	(0.102)	(0.113)	(0.116)
Internet (2G) * IS control	-2.699^{***}	-2.829^{***}	-2.777^{***}	-2.336^{**}
	(0.791)	(0.820)	(0.761)	(0.743)
Internet (2G) * Kurd control	-0.555^{*}	-0.907^{**}	-0.842^{*}	-0.865^{*}
	(0.276)	(0.351)	(0.338)	(0.354)
Internet (2G) * Opp control	0.033	-0.148	-0.040	-0.048
	(0.208)	(0.160)	(0.153)	(0.163)
# Killings (log)			-0.235^{***}	-0.236^{***}
			(0.058)	(0.059)
Govt gains				0.373
				(0.374)
Govt losses				-0.178
				(0.434)
Temporal FEs		✓	✓	✓
AIC	11642.420	9727.192	9496.747	9323.537
BIC	11687.097	9972.916	9746.939	9576.943
Log Likelihood	-5811.210	-4808.596	-4692.374	-4604.768
Deviance	9333.793	7328.565	7096.120	6975.761
Num. obs.	640	640	640	626

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Contested control. Governorate-clustered SEs.

Table A3. Internet accessibility (2G) and proportion of targeted killings. (Generalized linear regression, binomial with logit link).

A.2.3 Mobile phone access and state violence

	I	II	III	IV
Intercept	-2.468^{***}	-2.517^{***}	-1.247^{**}	-0.607
	(0.300)	(0.328)	(0.451)	(0.654)
Mobile Phones	0.218^{*}	0.240^{**}	0.199^{*}	0.190^{*}
	(0.096)	(0.091)	(0.089)	(0.091)
Govt control	0.703	0.863^{*}	1.262^{**}	1.251^{**}
	(0.441)	(0.388)	(0.403)	(0.413)
IS control	1.379^{*}	1.263	0.744	0.584
	(0.701)	(0.652)	(0.642)	(0.621)
Kurd control	1.025	1.572^{*}	1.004	1.037
	(0.562)	(0.640)	(0.630)	(0.640)
Opp control	0.215	0.576	0.249	0.311
	(0.574)	(0.509)	(0.486)	(0.487)
Mobile Phones * Govt control	-0.103	-0.166	-0.302^{*}	-0.293^{*}
	(0.141)	(0.125)	(0.131)	(0.135)
Mobile Phones * IS control	-1.241^{**}	-1.217^{**}	-1.102^{*}	-0.968^{*}
	(0.470)	(0.462)	(0.464)	(0.433)
Mobile Phones * Kurd control	-0.444	-0.764^{*}	-0.698^{*}	-0.720^{*}
	(0.263)	(0.326)	(0.313)	(0.321)
Mobile Phones * Opp control	-0.120	-0.311	-0.219	-0.243
	(0.221)	(0.179)	(0.171)	(0.171)
# Killings (log)			-0.211^{***}	-0.212^{***}
			(0.055)	(0.056)
Govt gains				0.475
				(0.393)
Govt losses				-0.118
				(0.442)
Temporal FEs		✓	✓	✓
AIC	11685.831	9744.918	9551.033	9368.747
BIC	11730.508	9990.641	9801.224	9622.153
Log Likelihood	-5832.916	-4817.459	-4719.517	-4627.373
Deviance	9377.204	7346.290	7150.406	7020.971
Num. obs.	640	640	640	626

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Contested control. Governorate-clustered SEs.

Table A4. Mobile Phone accessibility and proportion of targeted killings. (Generalized linear regression, binomial with logit link).

A.2.4 3-G Internet access (binary measure) and state violence

	I	II	III	IV
Intercept	-2.073^{***}	-2.126^{***}	-1.109^{**}	-0.492
	(0.148)	(0.226)	(0.341)	(0.541)
Internet access (3G binary)	0.346	0.372^{*}	0.327^{*}	0.310
	(0.177)	(0.168)	(0.161)	(0.165)
Govt control	0.805^{***}	0.670^{***}	0.789^{***}	0.788^{***}
	(0.148)	(0.181)	(0.178)	(0.180)
IS control	-0.248	-0.358	-0.646^{*}	-0.625^{*}
	(0.263)	(0.258)	(0.253)	(0.252)
Kurd control	0.159	-0.014	-0.368	-0.384
	(0.265)	(0.364)	(0.356)	(0.368)
Opp control	0.349	0.354	0.154	0.172
	(0.194)	(0.202)	(0.193)	(0.200)
Internet (3G binary) * Govt control	-0.482^{*}	-0.378	-0.528^{*}	-0.505^{*}
	(0.191)	(0.211)	(0.207)	(0.210)
Internet (3G binary) * Kurd control	-0.251	0.166	0.003	0.033
	(0.375)	(0.477)	(0.441)	(0.451)
Internet (3G binary) * Opp control	-0.690^{*}	-0.922^{***}	-0.727^{**}	-0.753^{**}
	(0.282)	(0.272)	(0.253)	(0.259)
# Killings (log)			-0.178^{***}	-0.179^{***}
			(0.047)	(0.048)
Govt gains				0.474
				(0.402)
Govt losses				-0.136
				(0.438)
Temporal FEs		✓	✓	✓
AIC	11752.861	9782.292	9597.306	9404.562
BIC	11793.070	10023.548	9843.030	9653.522
Log Likelihood	-5867.430	-4837.146	-4743.653	-4646.281
Deviance	9446.233	7385.664	7198.679	7058.786
Num. obs.	640	640	640	626

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Contested control. Governorate-clustered SEs.

Table A5. Internet accessibility (3G, binary measure) and proportion of targeted killings. Internet accessibility is coded 0, where there is no 3G Internet access, and 1 otherwise. (Generalized linear regression, binomial with logit link).

A.3 Further robustness tests

	I	II	III
Intercept	−0.761	−4.001**	−5.201***
	(0.557)	(1.445)	(1.187)
Internet access (3G)	0.255**	0.230*	1.236***
	(0.092)	(0.107)	(0.127)
Govt control (70%)	1.006**	0.224	0.268
	(0.316)	(0.450)	(0.153)
IS control (70%)	−0.589*	−1.014***	−0.916***
	(0.245)	(0.231)	(0.237)
Kurd control (70%)	−0.839	−0.337	−0.378
	(1.310)	(1.254)	(0.373)
Opp control (70%)	0.908**	−1.034	−0.485**
	(0.351)	(0.534)	(0.181)
# Killings (log)	−0.162**	−0.359***	−0.475***
	(0.059)	(0.074)	(0.069)
Govt gains	0.171		
	(0.331)		
Govt losses	−0.374		
	(0.404)		
Internet * Govt control (70%)	−0.309*	−0.113	
	(0.134)	(0.178)	
Internet * Kurd control (70%)	0.411	0.048	
	(1.011)	(0.926)	
Internet * Opp. control (70%)	−0.756***	0.850*	
	(0.189)	(0.418)	
Alawi		−1.407***	−0.802***
		(0.214)	(0.182)
Druze		−0.090	−0.244
		(0.153)	(0.139)
Kurd		−0.902*	−0.952***
		(0.377)	(0.239)
Christian		0.191	0.365**
		(0.160)	(0.113)
Pop (log)		0.528*	0.604***
		(0.235)	(0.178)
% Govt control			0.024***
			(0.004)
Internet * % Govt control			−0.017***
			(0.002)
Temporal FEs	✓	✓	✓
AIC	9359.577	7878.892	7294.457
BIC	9608.538	8146.954	7558.051
Log Likelihood	-4623.789	-3879.446	-3588.228
Deviance	7013.802	5470.264	4887.829
Num. obs.	626	640	640

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Control=Contested. Governorate-clustered SEs.

Table A6. Internet accessibility (3G) and proportion of targeted killings. A group is coded as in control if it controls more than 70% of a territory. Where no group controls more than 70%, control, control is coded as 'contested'. (Generalized linear regression, binomial with logit link).

	3G	lagged 3G	3G	lagged 3G
Intercept	-6.321^{***}	-5.679^{***}	-5.877^{***}	-5.140^{***}
	(1.434)	(1.482)	(1.440)	(1.562)
Internet	0.281^{*}	0.146	0.910^{***}	0.828^{***}
	(0.109)	(0.112)	(0.130)	(0.146)
Govt control	-1.192^{**}	-1.132^{*}	0.126	0.342
	(0.448)	(0.466)	(0.281)	(0.286)
IS control	-1.339^{***}	-1.329^{***}	-1.134^{***}	-1.123^{***}
	(0.239)	(0.241)	(0.249)	(0.252)
Kurd control	2.150	1.888	0.556	0.387
	(1.214)	(1.234)	(0.519)	(0.516)
Opp control	-1.153^{***}	-1.240^{***}	-0.336	-0.367^{*}
	(0.313)	(0.314)	(0.184)	(0.183)
# Killings (log)	-0.531^{***}	-0.520^{***}	-0.613^{***}	-0.621^{***}
	(0.076)	(0.075)	(0.082)	(0.085)
Alawi	4.563^{***}	4.287^{***}	2.541^{***}	2.120^{*}
	(0.750)	(0.859)	(0.698)	(0.859)
Druze	-0.640^{**}	-0.447^{*}	-0.115	0.067
	(0.205)	(0.193)	(0.241)	(0.233)
Kurd	-2.614^{***}	-2.464^{***}	-1.734^{***}	-1.563^{***}
	(0.371)	(0.367)	(0.328)	(0.342)
Christian	-0.404^{*}	-0.289	0.006	0.136
	(0.162)	(0.166)	(0.141)	(0.153)
Pop (log)	1.195^{***}	1.117^{***}	0.997^{***}	0.911^{***}
	(0.209)	(0.211)	(0.209)	(0.222)
Unempl. (%)	-0.025	-0.027^{*}	-0.013	-0.016
	(0.013)	(0.013)	(0.014)	(0.014)
Govt gains	0.231	0.159	0.421	0.379
	(0.336)	(0.337)	(0.373)	(0.370)
Govt losses	-0.417	-0.560	-0.170	-0.243
	(0.332)	(0.334)	(0.338)	(0.332)
Internet * Govt control	0.141	0.203		
	(0.151)	(0.158)		
Internet * Kurd control	-0.436	-0.323		
	(0.880)	(0.952)		
Internet * Opp. control	0.640^{***}	0.669^{***}		
	(0.168)	(0.164)		
Internet * Alawi	-1.724^{***}	-1.613^{***}	-1.041^{***}	-0.883^{***}
	(0.224)	(0.261)	(0.203)	(0.260)
% Govt control			0.010^{*}	0.010^{*}
			(0.005)	(0.005)
Internet * % Govt control			-0.011^{***}	-0.011^{***}
			(0.002)	(0.002)
Temporal FEs	✓	✓	✓	✓
AIC	7209.642	7308.245	7033.386	7141.687
BIC	7489.722	7588.325	7309.021	7417.321
Log Likelihood	-3541.821	-3591.122	-3454.693	-3508.843
Deviance	4849.866	4948.469	4675.611	4783.911
Num. obs.	626	626	626	626

$^{***}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$. Reference category: Control=Contested. Governorate-clustered SEs.

Table A7. Internet accessibility (3G and lagged 3G access) and proportion of targeted killings (Generalized linear regression, binomial with logit link). Models 1 and 3 account for 3G Internet access, and models 2 and 4 account for 3G lagged Internet access at t-1.

A.4 Relative effect sizes

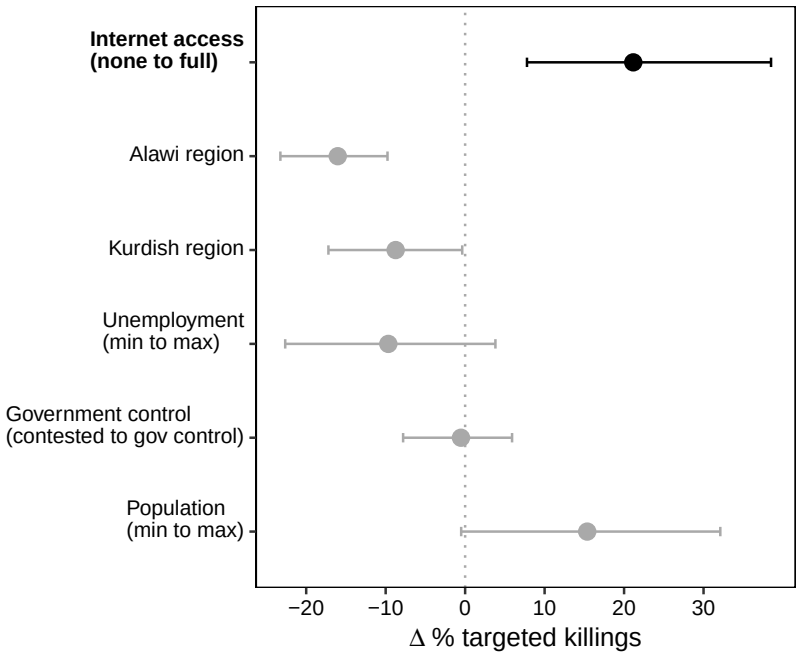


Figure A3. Expected change in proportion of targeted killings, given changes in individual explanatory variables.

Figure A3 offers a comparison of the substantive effect sizes for different factors that may be correlated with a governments repressive strategy.[23] For each variable, the expected change in the proportion of targeted killings is simulated by holding the remaining variables constant[24] and calculating the difference in proportion given a change in the variable of interest. All else equal, a change in Internet accessibility from no access to full access is followed by an average change in the proportion of targeted killings by about 20 percentage points.

In areas where the Alawi minority lives the proportion of targeted killings is roughly 15 percentage below other areas within Syria. Kurdish areas are also likely to experience a slightly higher proportion of indiscriminate violence. Changing levels of pre-war unemployment are not significantly correlated with changes in the strategy of violence used by the government. Although the model indicates a significant difference in the targeted repression in areas that are predominately controlled by the government, the expected percentage points change in targeted repression is not significantly different from zero. Finally, when holding all other factors equal, population size is not associated with a significant change in the percentage of targeted killings (at the 95% level).

The substantive changes in repressive strategy by the Syrian regime presented in Figure A3 suggest that Internet accessibility is not only significantly associated with higher proportions of targeted violence, but that changes in accessibility also coincide with substantive changes in the regime's repressive strategy, and these substantive changes are

[23]The simulations are based on model 6 in Table 1 in the main manuscript.

[24]I use the mean for continuous variables, and the median for binary variables.

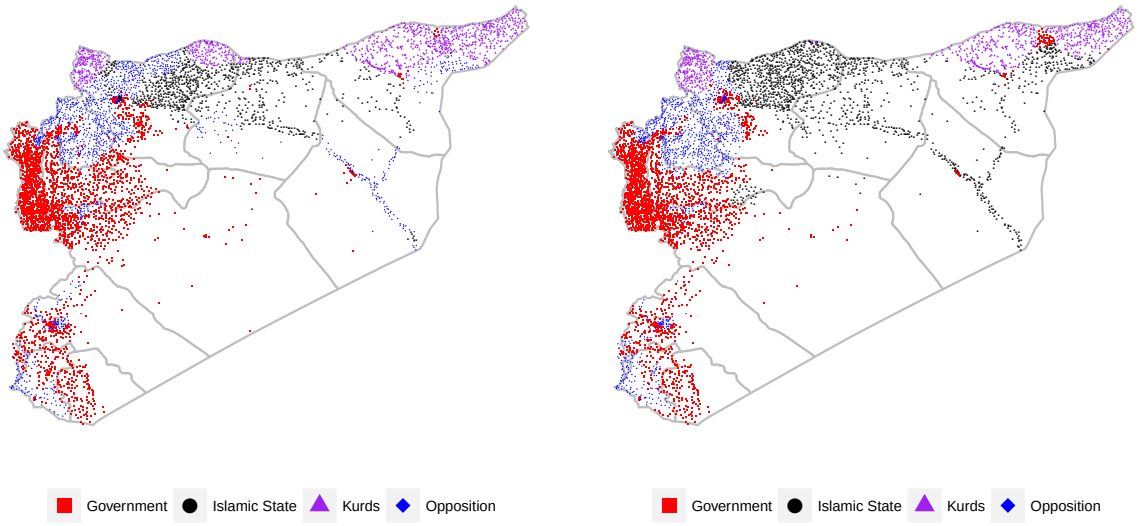
quite large, when compared to other important explanatory factors. While the Figure 4 reminds us that changes in accessibility are mediated by levels of territorial control, the simulated example here clearly demonstrates the importance of accounting for Internet connectivity if we want to understand how violent strategies are manifesting themselves in modern conflicts.

B Measuring Armed Group Presence/ Territorial control

To measure armed group presence, I rely on data collected by the Syria Conflict Mapping Project (SCMP) that is part of the Carter Center to construct an indicator of individual armed group presence and territorial control. Their sources include journalists, YouTube videos of live footage of the conflict, human rights organization, and stakeholders within the conflict, among others.[25].

Figure A4 shows the different factions controlling presence for January 2014 and January 2015, respectively. Red communities are controlled by Government forces, blue by the Opposition, black by Islamic State forces and purple areas are controlled by Kurdish forces, most notably the YPG. In Figure A4 the progression of Islamic State forces in both Al-Hasakah (the North-East) as well as Aleppo and Ar-Raqqah governorates are clearly visible. By January 2015 (Figure A4b) Islamic State forces have pushed out Kurdish forces from even larger parts of Aleppo, Ar-Raqqah and Al-Hasakah. But not only the Islamic State has gained ground in the Kurdish North-East territory, so have regime forces (as can be seen in red in the top right corner of the map).

[25] See https://www.cartercenter.org/peace/conflict_resolution/syria-conflict-resolution.html



(a) January 2014 (b) January 2015

Figure A4. Armed group presence in Syria - community level, January 2014 and 2015.

year	Government	Opposition	Kurds	IS
2013	55.55	27.81	7.13	9.57
2014	54.99	24.71	7.93	11.40
2015	50.34	23.26	6.48	18.33

Table A8. Yearly percentage of territory (by governorate) under control by each faction

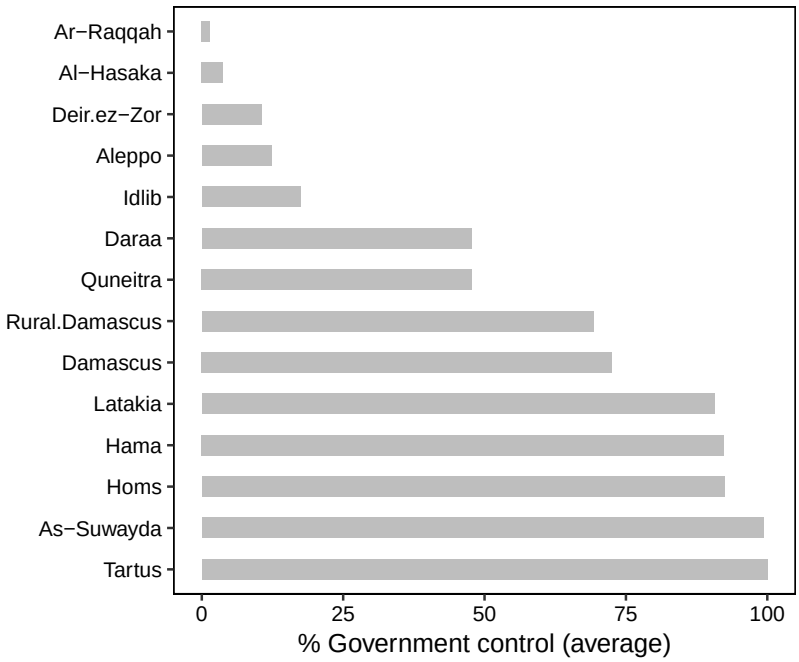


Figure A5. Average percentage of government control, by governorate.

To construct the categorical measure of control I calculate the percentage of communities controlled by each conflict faction for every two-week period and every governorate. For example, in Aleppo in the first two weeks of January 2014, Government forces controlled 13%, Kurdish forces controlled 22%, Opposition groups 32% and Islamic State forces controlled 34% of all communities. In January 2015, the proportions had changed to 11% Government, 15% Kurds, 22% Opposition and 51% Islamic State control in Aleppo.

C Measuring state violence in Syria

The following section describes the steps involved in creating a measure of state violence in Syria. In the first step, data on individual killings perpetrated in Syria that were collected by four different documentation groups are combined through record-linkage. In the second step, circumstantial details recorded on each killing found in the four different sources are combined to maximize the information available on each killing. Third, this information is used to classify whether an individual was killed in either a targeted or untargeted way, using supervised machine-learning for text classification. Fourth, the classified records form the basis of estimation models aimed at estimating the number of undocumented killings in each category (targeted or untargeted), to account for biases in the reporting process.

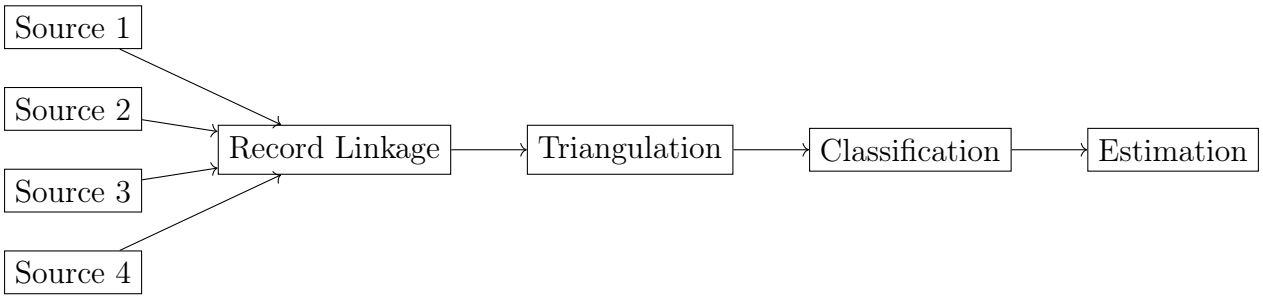


Figure A6. Data processing

The four data sources used are the following:

- Syrian Center for Statistics and Research. As described on its website, "The center includes a local network of reporters and a team of researchers and academics inside and outside of Syria."
- Damascus Center for Human Rights Studies. The Damascus Center for Human Rights Studies maintains several documentation projects in addition to lobbying and advocating for Syrian human rights and working to draw attention to the situation in Syria.
- Syrian Network for Human Rights. SNHR conducts monthly reviews of their records and subsequently updates their dataset with newly discovered or verified victims. SNHR maintains a website where they describe that they "adopt the highest approved documentation principles by the international bodies." Also available on

their website is a description of their three phase documentation process and the six categories of victims they document.

- Violation Documentation Centre. The "About" page of their website describes the data classification methods and three-stage data verification process implemented by the VDC.

C.1 Record-linkage

The record linkage process described here was conducted in collaboration with [anonymized]. The record-linkage project worked with data from 15 March 2011 through 31 December 2015. For the present manuscript, data from 1 June 2013 through 30 April 2015 was used. The following sections, first explained in (Price, Gohdes and Ball, 2016), describe the record-linkage process that was used for the entire data.

In order to know how many deaths have been documented, we need to identify the multiple records that refer to the same individuals. These records may be within the same list (e.g., the same source records the same victim multiple times, perhaps because he or she was reported by multiple community members) or across sources (e.g., different sources record information about the same victim). The records may contain impartial and imperfect information, and the records contain no unique identifying number such as a national id number. The challenge of deduplicating databases with imperfect information arises in a variety of contexts and has been studied across disciplines for decades. It is called "record linkage" when there are two databases, and "database deduplication" when there are three or more. Christen (2012) provides an overviews of the problem and various methods.

In our case, we begin with records of identifiable victims. An identifiable victim is a record that includes at least two words from the victim's name, plus the date and location of death. The full identifying information is essential for the comparisons required to match records to each other. Records lacking the complete information are considered "anonymous" and are excluded from the analysis. The anonymous records describe victims of violence in the Syrian Arab Republic who deserve to be acknowledged. However, they cannot be included in this step of the analysis because it is impossible to determine if the records with partial information refer to killings also described by other records. That is, anonymous records cannot be matched or de-deduplicated. Records with partial information provide hints about the existence of killings which have not been fully documented; estimating the number of *undocumented* killings will be performed in the last step on this process.

To identify multiple records that refer to the same individual, we employ a combination of human review and computer modeling. Humans review subsets of records—some in the original Arabic, others in translated English[26]—and combine groups of records that they believe refer to the same individual. Computer algorithms are then used to model the decisions the humans made, to assign a probability that any two records refer to the same individual. These probabilities are then used to cluster records into groups that

[26]We have found that these reviewers make highly comparable decisions, regardless of the language in which they review the records. See Section C.1 for details.

represent the information available about a single individual across all the data sources. This is called "semi-supervised" modeling.

Inter-Rater Reliability (IRR)

When two or more individuals review and code data, it is common to need to assess the consistency of the decisions made by those individuals. Formally, this assessment is referred to as inter-rater reliability (IRR) and is generally described using the overall percent agreement among coders and a kappa coefficient. There are a variety of other statistical measures to evaluate IRR, but kappa is commonly used for categorical measures, such as assigning match/non-match to groups of records.

First, the overall agreement rate is the proportion of times that multiple coders make the same decision. For example, for this project coders A and B each reviewed the same 63,249 pairs of records (coder A in English, coder B in Arabic) with overall agreement 96%. Coders B and C each reviewed the same 63,951 pairs of records (both working in Arabic) with overall agreement 95.4%. Finally, coders A (English) and C (Arabic) each reviewed the same 86,371 pairs of records, with overall agreement 94.7%.

Second, kappa is calculated as this agreement, adjusted to consider the amount of agreement that might be expected by chance. Specifically:

$$\kappa = \frac{p_a - p_c}{1 - p_c}$$

where p_a is the overall agreement and p_c is the amount of agreement expected by chance. p_c is calculated from the total number of matches and non-matches assigned by each coder. For the same combinations of coders described above, coders A and B have a kappa value of 0.813, B and C a value of 0.817, and A and C a value of 0.796.

In general, a kappa above 0.8 is considered very good, 0.6-0.8 is good, and 0.4-0.6 is considered moderate.

Perhaps even more important than the raw percent agreement and kappa values is the consistency of those values regardless of whether the coders being compared are both working in Arabic or one is working in English and the other Arabic. These results imply that the decisions made by each of the reviewers are highly consistent, regardless of whether they were reviewing the records with the original Arabic content or translated into English.

Hand-Labeled Data

We begin with all victims recorded by one or more of the documentation groups, regardless of the circumstances of their death. As a result, we begin with 413,954 total records of victims. It is important to note that this number refers to the total number of records prior to matching and de-duplication—it should *not* be inferred to indicate the total

number of victims killed in the ongoing conflict. This count includes many examples of duplicated information.

From this set of total records, we selected small groups of records with similar names, locations, and dates of death, which a human reviewer sorted into even smaller groups of records, called clusters, in which all the records in each cluster refer to the same person. From these clusters we can identify pairs of records that refer to the same person ("positive pairs" or "matches", of which there were 128,741 pairs) and pairs of records that do *not* refer to the same person ("negative pairs" or "non-matches", of which there were 427,638 pairs). It is useful to organize records as either clusters or sets of pairs for various different steps in the record linkage process. These human-labeled pairs and clusters are used to evaluate decisions in the next step (blocking) and to train the pairwise classification model described in the classification step.

Blocking

In order to link records that refer to the same person, we create a model that estimates the probability that any *pair* of records refer to the same person. Rather than estimate this model on the full combination of all possible pairs (which would be approximately 85 billion pairs), we limit the consideration to only the pairs that have a reasonable chance of being matched. This process of limiting the analysis to a subset of pairs is called "blocking" or "indexing."

In brief, we consider the total number of positive pairs identified in the hand-labeled data, looking for combinations of common field values that define subgroups ("blocks") within which all the positive pairs are found.

This approach covered all but 0.4% of the hand-labeled positive pairs and generated a total of 44,448,855 pairs. This is the set of pairs that must be considered in the remaining steps.

Feature Definition

The primary bases for comparing records are the name of the victim, and the date and location of the death. In order to represent the similarities and differences among records, there are many possible comparisons among these fields, including whether the values in a field in two records are exactly equal, or much more complicated comparisons. According to the pairwise classification models that we have considered, the most useful comparisons for determining matches/non-matches are:

- Given a list of all the names (in English and in Arabic), sort them alphabetically, then calculate the number of deletions and insertions required to transform one into the other (called the Jaro-Winkler distance). This is an edit distance normalized to the length of the string.

- Calculate the number of first, middle, and last names common to both records divided by the total number of names in either record (called the Jaccard index). Calculated for both English and Arabic versions of the names.
- The Jaccard index for the words in the location descriptions (in Arabic).
- Whether the names share substrings (measured by locality sensitive hashing, see Rajaraman and Ullman (2011, ch. 3)), the first five characters, or the last five characters (in Arabic).
- The number of days between the two dates of death.
- Whether the year, month, and governorate are exactly the same.[27]

We found a total of 32 comparisons to contribute substantially to the probability of matching. These comparisons are the "features," or predictor variables, used in the pairwise classification of whether a given pair is or is not likely to be a match.

Pairwise Classification

The hand-labeled data, both positive and negative pairs, was randomly divided into two groups, one for training with 440,464 "training" pairs, and a second group of 115,915 pairs used for testing. The training records were given to a "gradient boosted trees", or "xgboost" algorithm[28], and the resulting model was used to classify the testing data.

Note that the pairs in the training and testing sets are "hard." That is, we did not include pairs that are obviously non-matches, and many of the matches are pairs with slightly different dates or names. The classification was nonetheless quite accurate.

Combined, the confusion matrix creates a mean positive-negative F_1 score of 0.917. Another way to evaluate a pairwise classification model is through the calculation of a Brier score. In our case this metric suggests that on average, the classification scores are approximately 0.23 away from the hand-labeled values of zero (for non-match) or one (for a match).

The model was applied to the 44,448,855 pairs generated by blocking; each pair was assigned a probability of being a match.

Clustering

Once the records are classified, we need to decide which groups of records refer to the same person; together, the records that refer to a single person are called a *cluster*. There may be one, two, or more records in a cluster.

[27] The location information is restricted to the governorate level, as more fine-grained location information was only collected in an unsystematic way, and can therefore not be compared and analyzed across sources.

[28] The implementation described here: http://xgboost.readthedocs.io/en/latest/.

Our approach first partitions the records into groups via transitive closure, linking all the pairs which have even a small probability of being matches (a classification score > 0.4) into a super-cluster, called a "connected component."

We next separate each connected component into smaller clusters which maximize the similarity of the records to each other using a method called "hierarchical agglomerative clustering" (HAC). [29]

Merged Records

For clusters with more than one record, the information across all the records must be merged to form a single, unified record. For a few groups of records, this means that contradictory information from different records that refer to the same person must be resolved. When there are multiple records in a cluster with differing values, the most common (nonmissing) value for each field is chosen; ties are broken by random selection.

C.2 Triangulation

In the second step, circumstantial details recorded on each killing found in the four different sources is combined to maximize the information available on each killing.

Figure A7 presents a model of this triangulation process for an individual record: Assuming that a violent event was documented by three of the four groups, we can combine the notes on death circumstances from these three sources to arrive at a more nuanced understanding of how (and possibly why) this person was killed by the government. These combined, or 'aggregated' texts form the basis on which the classification of records is conducted. The aggregated information for the record presented in Figure A7 indicates that this person was tortured and shot while in custody with the Air Force Intelligence branch in Hama airport, after having been arrested previously.

[29] Specifically, we use an average weighting method and a threshold-based cluster flattening, with $t = 0.4$. This is a distance measure rather than similarity measure, so it is slightly more strict than the threshold used in transitive closure.

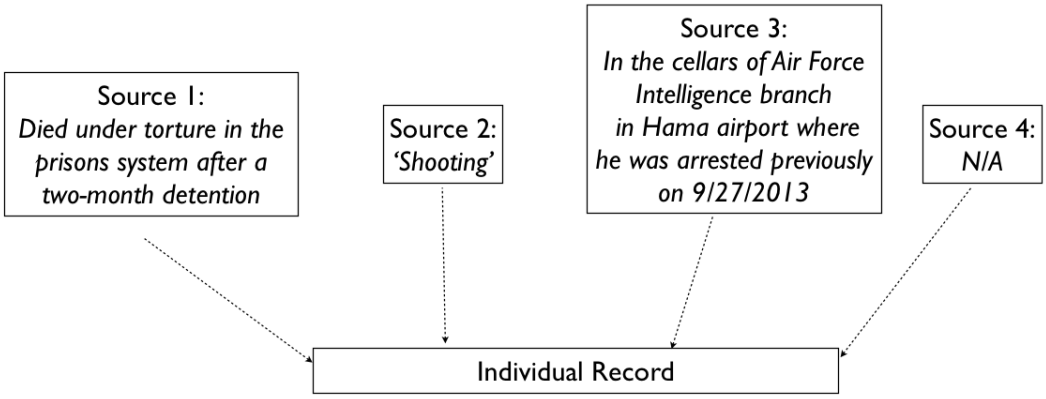


Figure A7. Assembling information on record details

C.3 Classification of killings

In the third step, the triangulated information is used to classify whether an individual was killed in either a targeted or untargeted way, using supervised machine-learning for text classification. The information provided by the four human rights groups was translated from Arabic into English using the Google Translate API.

I use supervised machine-learning to classify the over 65,000 aggregated reports on individual killings that were committed by the Syrian regime (and pro-government forces) between June 2013 and April 2015. In the hand-coded training set, 2347 records are classified by hand. The overwhelming majority of records could be unambiguously assigned to each category. For the few records where the description did not yield a clear indication of whether the killing was targeted or untargeted, I conservatively coded them as untargeted.

Of the over 60,000 records analyzed by the classifier, only 162 included no reported details, which were all classified as untargeted killings. 3695 records only included a one word descriptor, of which 3338 records reported the killing as a 'shooting', and 141 as a 'shelling'. All records that included a one-word descriptor that said 'shooting' , 'shelling', or 'clashes' were also classified as untargeted killings.

The results presented in the paper use the gradient booster *xgboost* (Chen and Guestrin, 2016; Chen et al., 2017) to classify the records according to these categories. A variety of different algorithms were tested, including support vector machine-learning and random forest models, however, as A9 show, the extreme gradient booster provides the highest overall algorithm performance. The classification process was performed using the `xgboost` and `RTextTools` R packages (Chen et al., 2017; Jurka et al., 2012).

Classifier	Accuracy	Category	Precision	Recall
SVM	0.93	Untargeted	0.92	0.92
		Targeted	0.85	0.88
		Other	0.94	0.93
Random Forest	0.94	Untargeted	0.91	0.93
		Targeted	0.90	0.86
		Other	0.95	0.96
xgboost	0.93	Untargeted	0.93	0.93
		Targeted	0.90	0.92
		Other	0.94	0.92

Table A9. Out-of-sample performance of classifiers

Table A10 show the N-grams with highest feature importance for each category. It shows that the features reflect the conceptual distinctions very well.

Untargeted	bombing, clashes, shelling, shooting, bombardment, result, regime, city, help, ad, ambush, martyrdom, abdullah, died, citing, east, abu, aka, massacre, carrying, front, indiscriminate, assassination, military, baadaguethamanm
Targeted	torture, sniper, executed, snipers, prison, arrest, dissident, knives, kidnapped, security, burning, defector, shabiha, field, activist, slaughtered, prisons, dead, cellars, bound, shot, flee, trying, hands, storming
Other	state, iraq, execution, pkk, islamic, al-baghdadi, explosion, islam, clan, levant, number, found, ongoing, organization, hospital, organizing, sham, union, free, people, car, brive-class, village, al-islam, control

Table A10. N-grams with highest feature importance for each category

Figure A8 shows the distribution of probabilities for each classified record as being targeted.[30] The y-axis is capped at 10,000 records in order to facilitate the examination of the probabilities further away from the extremes, which would indicate that the algorithm is not well able to discriminate between the different categories. The graph shows that the classifier is able to discriminate between types of killings very well. Of the more that 60,000 records classified, only a very small number fall between the two extremes. If we look at the number of classified cases that were labeled as targeted where the assigned probability is smaller than 95%, and the classified cases that were labeled as being untargeted killings where the assigned probability of being targeted is more than 5% (in other words the cases that fall between the extreme outer values on the x-axis), we see that these only constitute 5,2% of all classified records.

[30]The records classified as 'other' are not shown as it only concerns a small number of records and would make the interpretation less straightforward.

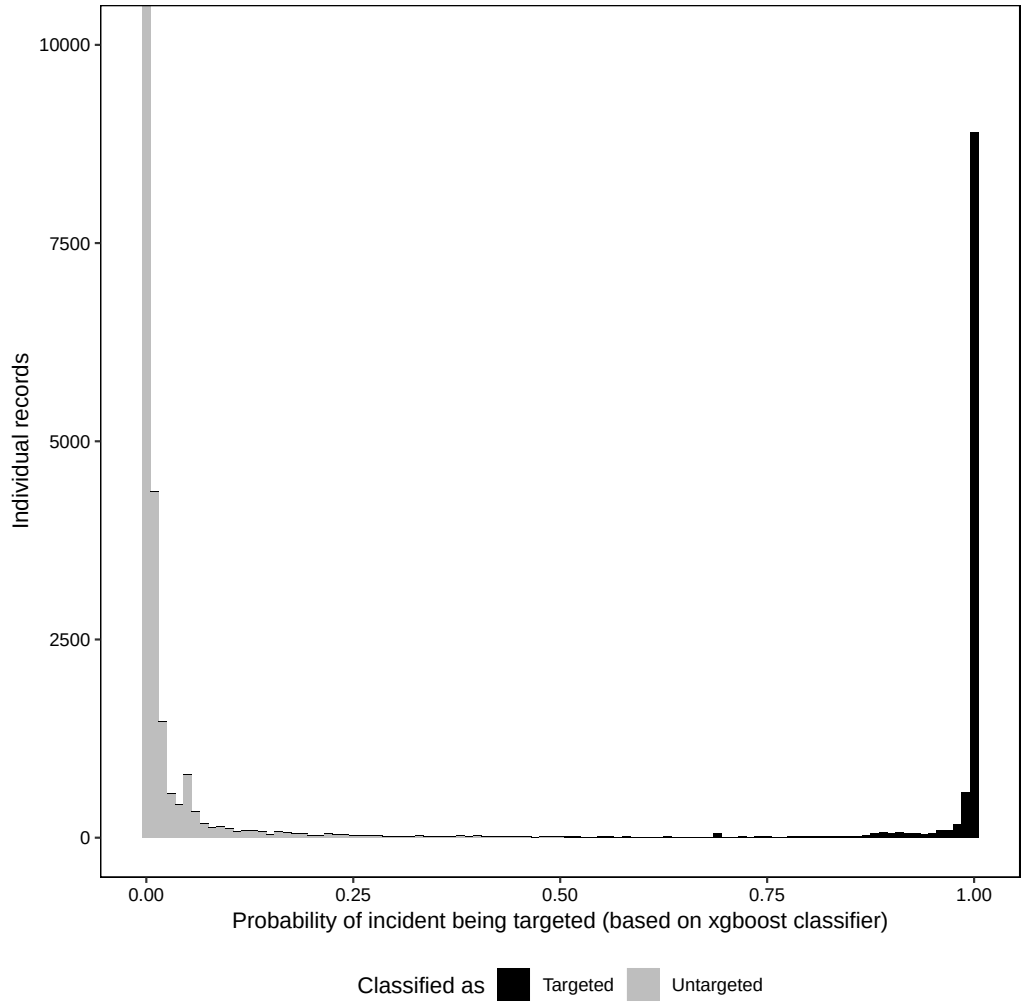


Figure A8. Histogram of probabilities for each record being either targeted or untargeted. Y-axis cut at 10,000.

Table A9 shows the number of words available for each individual record of killing, both by classified type of violence, and by governorate. If the number of words varied dramatically across violation types or across regions this may be an indication for an unequal amount of reporting on the documented killings in the database. Across governorates the amount of information reported looks quite consistent - with the minor exception of untargeted killings in As-Suwayda, Latakia, and Tartus, which all have slightly fewer words reported for these categories.

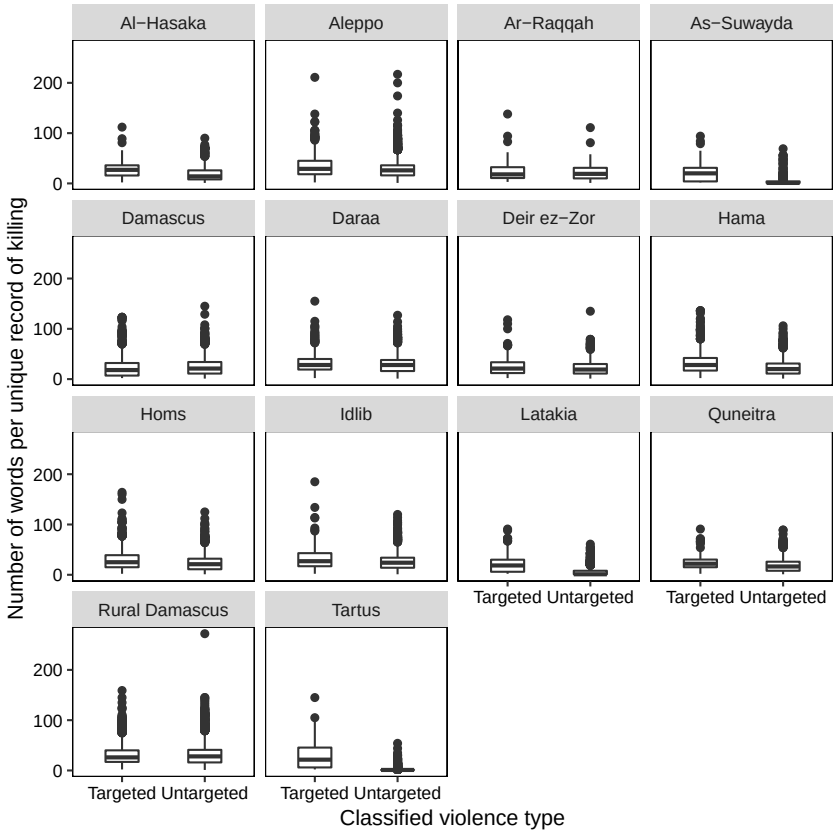


Figure A9. Number of words describing each individual record of killing, by classified type of violence and governorate.

Table A11 presents the details of death of randomly selected records, as well as their associated classification category. Post-classification, five records were randomly selected for each classified category in order to see examples of text associated with the three established classes of killings. Thus, while Table A10 shows us the words with the highest feature importance in the training set, Table A11 shows us randomly selected examples classified by the machine-learning algorithm.[31].

[31]Note that the text does not include punctuation, is translated to English from Arabic, which explains terms such as 'forces of the order' for regime forces, and other words that are direct translations from Arabic words, and is frequently repetitive as it includes collated information from up to four different sources (see Section C)

Untargeted	1: shot dead by the forces of order clashes with the forces of order spent during the clashes with the forces of order on the front of basil of the free army spent during clashes with regime forces on the front basil he was killed during the clashes with the regime s army forces shooting 2: as a result of aerial bombardment by shelling with rockets on the town stereochemistry by the bombing of the forces of order to the rocket interstitial esctahed shelling 3: by shelling of the city shelling cited by the bombing of army forces shelling 4: he was killed during the clashes with the regime s army forces on the front of the land of al dahr near the barrier alfajokh shooting 5: martyred during clashes
Targeted	1: killed under torture martyred under torture in prisons system the date of death is unknown precisely arrest torture 2: martyred under torture in prisons in the branch system arrest torture 3: killed under torture after the arrest of nearly two years where he worked in greenhouses he was killed under torture in the prisons of the regime as long as two years after the arrest the date of death is not known accurately arrest torture 4: martyred under torture in prisons system arrest torture 5: martyred under torture in prisons system according to information five days before his martyrdom arrest torture
Other	1: he was found dead near the mill faisal it is noteworthy that the area was under the control of the organization of the state of sham and iraq was buried in tel lifted discovery of a mass grave containing the body of a twenty faisal at the mill which was under the control of the organization of the islamic state in iraq and the levant nk was buried in tel lifted surnamed b abu zafer kidnapping execution 2: martyred during clashes with the islamic state forces in iraq and the levant nk shooting 3: martyred during clashes shooting he was killed during the clashes with the pkk forces and was buried in garihtaianh shooting 4: he spent more than civilians were slaughtered and burned to death with a knife and an execution ground in a massacre by the organization of the state islamic attack in iraq and the levant on alambauajjh village in the eastern city of peaceful countryside hama the execution of field 5: documented in the death of approximately armed element during the clashes between the free syrian army and the organization of the islamic state in iraq and the levant nk shooting

Table A11. Post-classification: Five randomly selected record details for each classified category (xgboost model)

The first five examples are records labeled by the classifier as untargeted killings. The first refers to an individual who was killed through shooting in clashes with regime forces. The second and third record refer individuals who were killed by shelling/aerial bombardment. The fourth and fifth record refer again to clashes. The second section of records were labeled by the classifier as targeted killings. All five records refer to individuals who were killed under torture within the Syrian prison system. Some records include further information (such as how long the individuals had been arrested beforehand), while others only mention the fact that they died in prison under torture. The final five records were labeled by the classifier as 'other' cases. Recall that this category was intended to detect killings that were not perpetrated by the regime. The first, second, and fourth records mention that the killing occurred in territory controlled by Islamic State fighters, and

during classes with the Islamic State.[32] The third record refers to an individual that was killed in clashes with the PKK. The final record mentions that the individual was killed in clashes between the Free Syrian Army and the Islamic State.

Overall, the randomly selected example records and their associated classified 'types of violence' suggest that the classifier is assigning labels in the same way a human coder would. Due to the focused vocabulary used to describe the details of death for each record, both the out of sample performance of the classifier based on the hand-classified data, as well as the short post-validation of classified records performed here show that the classification of violation types works very well.

C.4 Estimating undocumented killings

By merging the multiple records that refer to the same individual, I create a single list with one row for each uniquely identifiable victim. The row contains information about which source(s) recorded information about that victim. The number of victims documented by a single source, by each possible combination of two sources, three sources, and all four sources, provides insight into the size of the total victim population. Multiple recapture estimation thus fits a model of the reporting process, based, in this case, on four sources of reporting, in order to predict what went unreported.

There exist a multitude of different statistical solutions for the multiple-recapture approach that address different problems associated with the samples to be included in the analysis (International Working Group for Disease Monitoring and Forecasting, 1995). Some documentation groups collecting information make use of the same local informants, which can lead to postive source dependencies. Furthermore some victims are killed in a more visible way than others (e.g. when victims are publicly executed) and will be more likely to be included in all lists, again leading to positive list dependency.

To deal with uncertain list dependencies, I use a model developed by Madigan and York (1997). The model is implemented in the `dga` package in R (Johndrow, Lum and Ball, 2015), and prevents the estimates of undocumented violence from becoming implausibly large, as is oftentimes the case when using conventional log-linear Poisson models. The model uses bayesian model averaging (BMA), which means that it averages over all possible dependence structures according to weights that are based on how well each structure fits given the data. In this model the list intersections between the different sources are specified to follow a multinomial distribution with a hyper-Dirichlet distribution as a prior. This approach uses Bayesian model averaging (Hoeting et al., 1999) to incorporate uncertainty about potential relationships between the lists.

For the purpose of this study, it is particularly important to discuss dependencies in reporting patterns that pertain to differing information access. Internet accessibility may increase information access, thereby allowing for a higher level of reporting where the Internet is accessible (Weidmann, 2016). I address this possible source of underreporting

[32]Note that Islamic State is frequently referred to as the Islamic State of Iraq and al-Sham, or Islamic State of Iraq and the Levant

by estimating separate multiple recapture models separately for each time period, governorate, and violation type (targeted vs. untargeted) under investigation (see Sekar and Deming, 1949). This process is called stratification. Multiple recapture estimation then attempts to find the model that best describes the process of reporting for each individual stratum. For example, this means that the number of targeted killings in Homs are estimated separately for each two-week period. If the level of overall reporting in Homs changes from one time period to the next, then the multiple recapture model that best describes the process of reporting will also change from one time period to the next. Through the process of stratification, as well as the incorporation of list dependencies, I therefore attempt to account for changes in reporting, for example due to changes in Internet accessibility, in a systematic way.[33]

C.5 Descriptives: Proportions of observed and estimated targeted and untargeted violence

Figure A10 shows the observed and estimated killings for both targeted and untargeted violence. It shows that although far fewer victims are killed in a targeted way, targeted killings have a higher probability of being reported than untargeted killings. The estimates show that the unreported dark figure of killings that were conducted in an indiscriminate way is significantly larger. Based on the best estimate for both types of killings, the evidence suggests that 17.8% of all targeted killings were not reported, while 24.6% of all untargeted killings were not reported. Relying on reported event counts would slightly overemphasise the occurrence of targeted killings. In the observed data on killings, just over 17% of all state-perpetrated killings are classified as targeted killings. When accounting for unreported killings, the ratio is slightly reduced to 16%.

The overall proportion of targeted versus untargeted violence follows the conventional understanding that in civil conflict, the majority of violence that is perpetrated is not directly targeted in nature (Kalyvas, 2006). Very little research, however, explicitly compares absolute numbers of targeted and untargeted violence perpetrated by the same actor (for an exception see Bhavnani, Miodownik and Choi, 2011). As discussed in the article, the operationalization of both targeted and untargeted killings is highly conflict and actor specific. For example in the context of the Northern Ireland conflict small-scale bombings were used by the provisional IRA to directly target their enemies (Heger, 2015). In Colombia, displacement was used as a strategic form of collective targeting of 'disloyal' citizens (Steele, 2011). In Syria, reports have continuously highlighted the use of barrel bombs and bombardments by the government as a means of indiscriminately killing civilians (Pinheiro, 2015). An important consequence of these context and actor-specific strategies of targeted and untargeted violence is that proportions of targeted and untargeted violence are likely to vary widely across conflicts. For example, strategically targeted bombings are likely to nevertheless produce a higher number of targeted killings than individual strategic disappearances of opposition leaders. Proportions of targeted

[33]Note that stratification only addresses issues of known capture heterogeneity for which covariate information is available (such as time, place, and violation type in this paper) (Johndrow, Lum and Manrique-Vallier, 2016, 2).

and untargeted violence, as well as overall levels of violence, are furthermore likely to be dependent on the conflict actor's military and economic strength.

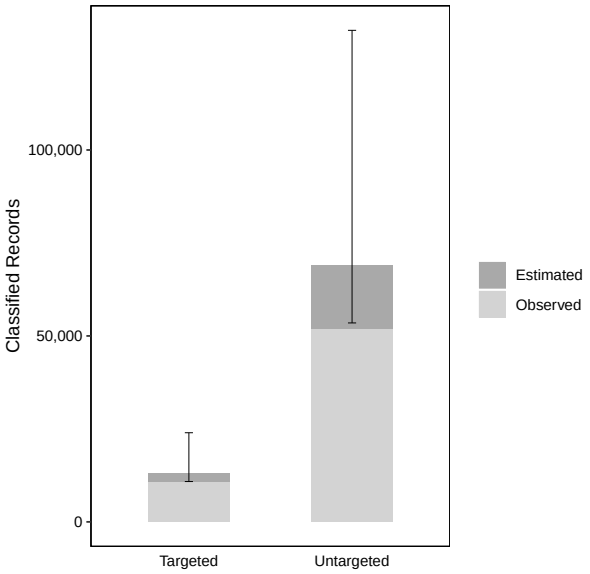


Figure A10. Targeted and untargeted violence, observed and estimated counts.

C.6 Descriptives: Dynamics of targeted and untargeted violence

Figure A11 shows the dynamics of targeted and untargeted violence over time, using the same time units as the analysis does (2-week intervals). The graph shows the variation in the different types of violence over time, as well as the variation in underreporting of violence for both types of violence. While the numbers are presented at the country-level, defining events of the conflict coincide with changes in the pattern of violence. It also suggests that patterns of targeted and untargeted violence do not merely coincide with each other, instead there are distinct dynamics to be found in both types of repressive strategy. In the second half of August 2013, a chemical attack generally attributed to the Syrian regime was perpetrated in Eastern Ghouta on the outskirts of Damascus, which led to a sharp increase in casualties resulting from this indiscriminate attack on civilians' lives. Figure A11 displays a sharp rise in the number of untargeted killings in the second half of August 2013. No comparable increase is discernible in the dynamics of targeted killings, which matches the key events of this time period.

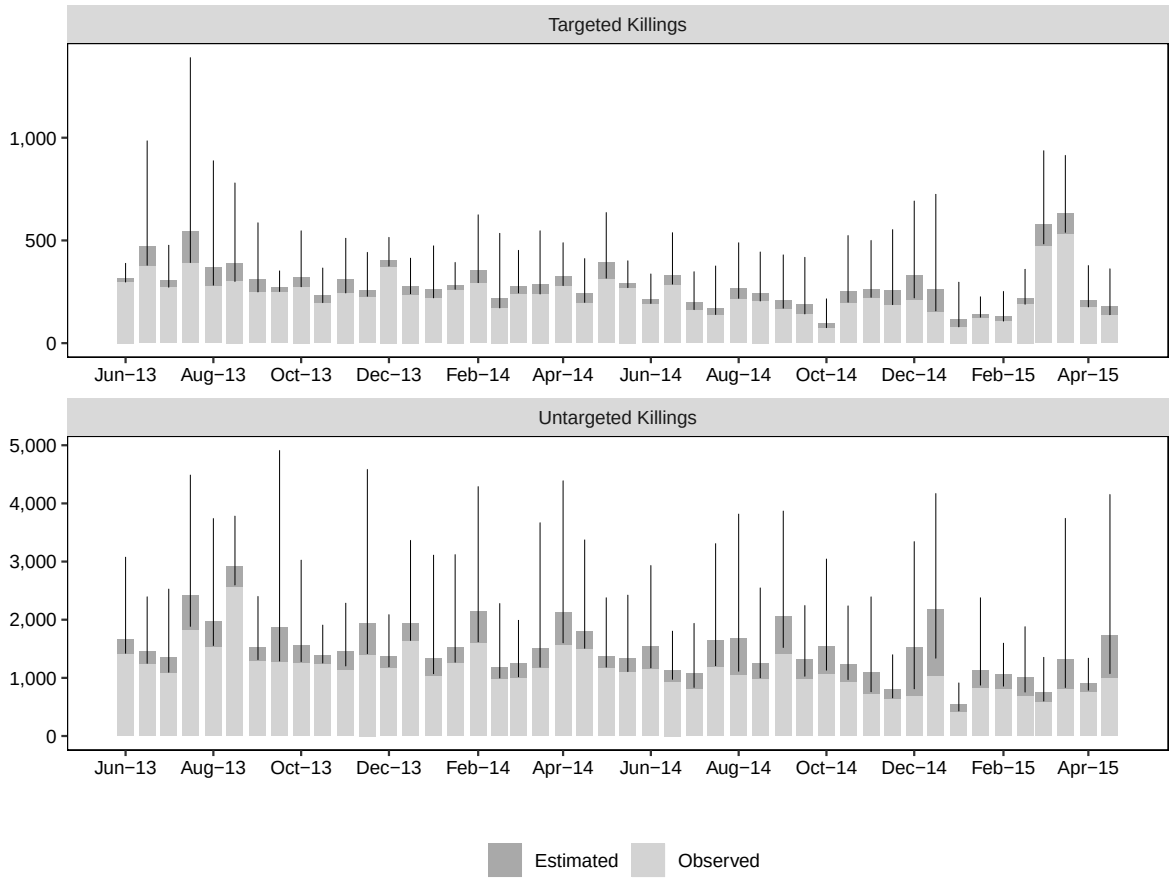


Figure A11. Targeted and untargeted violence, observed and estimated counts, over time.

A further notable dynamic is visible in December 2014. While there is a small increase in targeted violence, the estimates suggest that there was a noteworthy increase in untargeted violence in the last month of 2014. This increase was, however, less documented than previous levels of violence, as indicated by the fact that the darker part of the bar increases quite substantially in the first and second half of December 2014, when compared to November, and to January 2015. A closer look at the data reveals that the biggest increases in state violence at this time are to be found in Aleppo. Aleppo, located in the Northwest of Syria was at the end of 2014 an area that witnessed some of the most intense fighting in the entire country (The Carter Center, 2015). On the events in December, The Carter Center reports:

> In mid-December, government and pro-government forces broke through opposition lines and engaged opposition positions in Handarat Camp. The push placed government forces within 3 km (2 mi) of the last opposition-controlled highway into Aleppo city, and approximately 6 km (4 mi) from government positions on the eastern side of Aleppo city (The Carter Center, 2015, 7).

The spike in violence visible in the data suggests that the breaking of opposition lines was accompanied with substantial increases in untargeted violence, but that due to the intensity of the situation and the number of conflict actors simultaneously present in Aleppo, documentation work was not as able to fully keep up with the level of violence. The

difference between documented and estimated violence presented here further supports the need for working with estimated levels of violence, as documentation may not be able to keep up with events on the ground.

A final noteworthy dynamic is the increase in targeted killings in March 2015, a change that is not found in the levels of untargeted violence. A closer look at the data reveals that the majority of this increase in targeted violence in March 2015 is perpetrated in Damascus, and the region surrounding it (Rural Damascus). According to reports by the Syrian Observatory of Human Rights, a large number of opposition fighters defected to the Syrian Army in Southern Damascus in March 2015. Evidently the surrendering of insurgent fighters was accompanied by increases in targeted violence in Damascus, as well as the area immediately surrounding it (Al-Khalidi, 2015). Overall, a regaining of territory by the government, and an increase in defections by anti-government groups is associated with a significant increase in targeted killings in March 2015.

References Supporting Information

Al-Khalidi, Suleiman. 2015. "Seventy insurgents defect to Syrian army in Damascus suburb." *Reuters World News* . (accessed 14 January 2019).
URL: *https://www.reuters.com/article/us-mideast-crisis-defections/seventy-insurgents-defect-to-syrian-army-in-damascus-suburb-idUSKBN0M722D20150311*

Bhavnani, Ravi, Dan Miodownik and Hyun Jin Choi. 2011. "Three Two Tango: Territorial Control and Selective Violence in Israel, the West Bank, and Gaza." *Journal of Conflict Resolution* 55(1):133–158.

Chen, Tianqi and Carlos Guestrin. 2016. Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*. ACM pp. 785–794.

Chen, Tianqi, Tong He, Michael Benesty, Vadim Khotilovich and Yuan Tang. 2017. *xgboost: Extreme Gradient Boosting*. R package version 0.6-4.
URL: *https://CRAN.R-project.org/package=xgboost*

Christen, Peter. 2012. *Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection*. New York: Springer.

Heger, Lindsay L. 2015. "Votes and violence: Pursuing terrorism while navigating politics." *Journal of Peace Research* 52(1):32–45.
URL: *https://doi.org/10.1177/0022343314552984*

Hoeting, Jennifer A., David Madigan, Adrian E. Raftery and Chris Volinsky. 1999. "Bayesian Model Averaging: A Tutorial." *Statistical Science* 14(4):382–417.

International Working Group for Disease Monitoring and Forecasting. 1995. "Capture-recapture and multiple-record systems estimation I: History and theoretical development." *American Journal of Epidemiology,* 142:1047–1058.

Johndrow, James E, Kristian Lum and Daniel Manrique-Vallier. 2016. "Estimating the observable population size from biased samples: a new approach to population estimation with capture heterogeneity." *arXiv preprint arXiv:1606.02235* . (accessed 2018-10-15).
URL: *https://arxiv.org/abs/1606.02235*

Johndrow, James, Kristian Lum and Patrick Ball. 2015. "dga: Capture-Recapture Estimation using Bayesian Model Averaging.".
URL: *https://cran.r-project.org/web/packages/dga/index.html*

Jurka, Timothy P., Loren Collingwood, Amber E. Boydstun, Emiliano Grossman and Wouter van Atteveldt. 2012. "RTextTools: Automatic Text Classification via Supervised Learning. R package version 1.3.9.".
URL: *http://CRAN.R-project.org/package=RTextTools*

Kalyvas, Stathis. 2006. *The Logic of Violence in Civil War.* New York: Cambridge Univeristy Press.

Madigan, David and Jeremy C. York. 1997. "Bayesian Methods for Estimation of the Size of a Closed Population." *Biometrika* 84(1):19–31.

Pinheiro, Paulo Sérgio. 2015. "The use of barrel bombs and indiscriminate bombardment in Syria." *Independent International Commission of Inquiry on the Syrian Arab Republic* . (accessed 20 November 2018).
URL: *https://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/CoISyriaIndiscriminateB*

Price, Megan, Anita Gohdes and Patrick Ball. 2016. "Technical Memo for Amnesty International Report on Deaths in Detention." *Human Rights Data Analysis Group* . (accessed 2018-07-01).
URL: *https://hrdag.org/wp-content/uploads/2016/08/HRDAG-AI-memo-2.pdf*

Rajaraman, Anand and Jeffrey D. Ullman. 2011. *Mining of Massive Datasets.* London: Cambridge Univ Press.

Sekar, Chandra C. and Edwards W. Deming. 1949. "On a Method of Estimating Birth and Death Rates and the Extent of Registration." *Journal of the American Statistical Association* 44(245):101–115.

Steele, Abbey. 2011. "Electing Displacement: Political Cleansing in Apartadó, Colombia." *Journal of Conflict Resolution* 55(3):423–445.
URL: *http://jcr.sagepub.com/content/55/3/423.abstract*

The Carter Center. 2015. "Syria Countrywide Conflict Report No. 5.". (accessed 2018-12-19).
URL: *https://www.cartercenter.org/resources/pdfs/peace/conflict_ resolution/syria-conflict/NationwideUpdate-Feb-28-2015.pdf*

Weidmann, Nils B. 2016. "A closer look at reporting bias in conflict event data." *American Journal of Political Science* 60(1):206–218.