Repression technology: Internet accessibility and state violence

Anita R. Gohdes[*]

accepted at *American Journal of Political Science*

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.

[*] Email: gohdes@hertie-school.org. 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, Patrick Ball, Sabine Carey, Dara Cohen, Chris Fariss, Kelly Greenhill, Stathis Kalyvas, Jason Lyall, Will Lowe, Megan Price, Will Moore, Livia Schubiger, Lukas Stötzer, 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 21st 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 (Tufekci, 2017; Steinert-Threlkeld, 2017). In addition 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 (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 the 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. I expect that digital surveillance will be particularly useful for governments in areas that are not fully under their 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

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

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 Internet accessibility, and a variety of different model specifications. The findings highlight the ambiguous 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 the banning and alteration of individual media content. Overly zealous restriction has the potential of backfiring, when 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 states' 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 explicitly criticises 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-neighbouring 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 potential participants anticipated 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 early and in a precise way, and provide governments with an opportunity to target dissidents who have either organized dissident activities in the past, or 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 governments to further isolate groups from their core support network. In contentious contexts where opposition groups resist or even actively fight the government, garnering 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 increasingly rely 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 the 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 to 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 under 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 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 to 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 limited, it is limited intentionally, and where it is not 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 victim 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, 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 (see Price, Gohdes and Ball, 2016).

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.

[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.

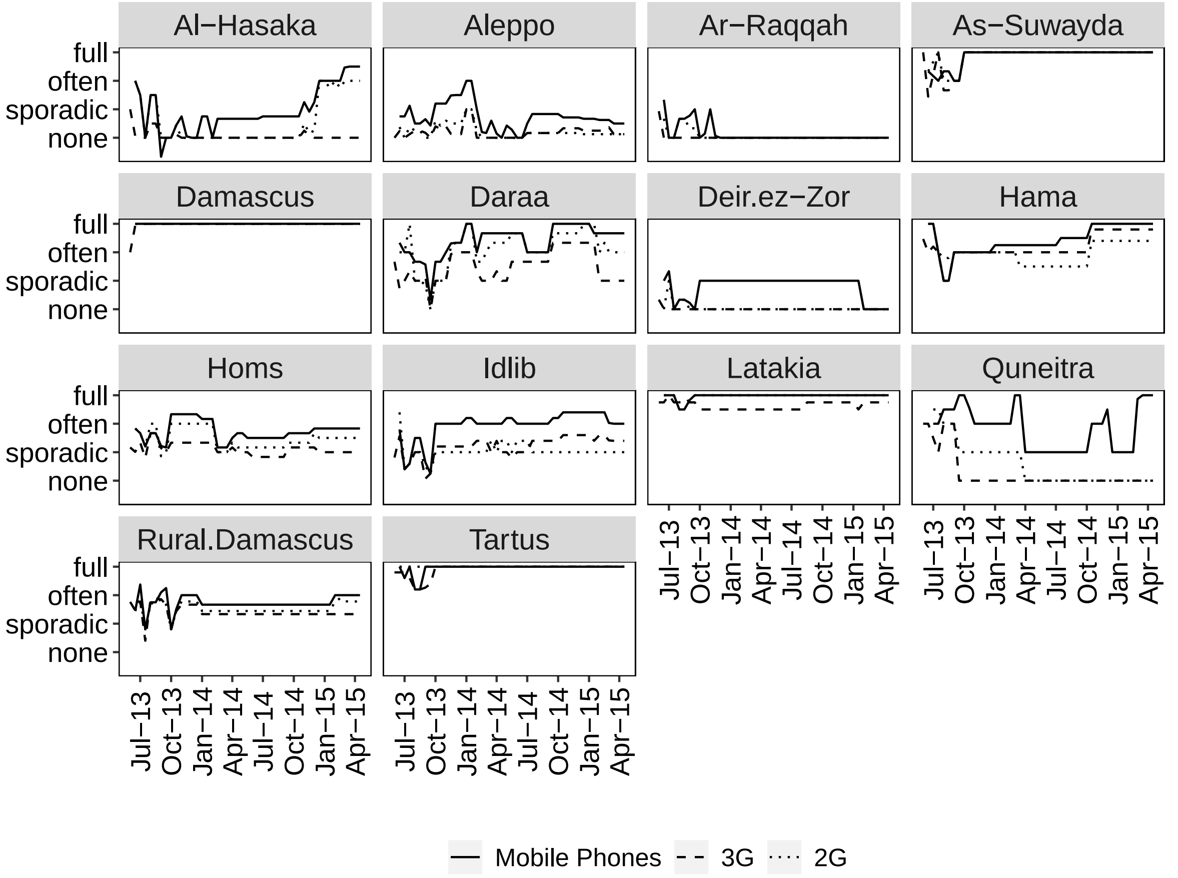

Figure 1. Network (mobile phones, 3G, and 2G) accessibility by Syrian governorate, June 2013 - April 2015.

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. Some areas, such as Tartus, which is predominately government controlled, and Damascus, which has been mostly 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 (Al-Hussien, 2017). 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 most accurate and detailed open source information on conflict events occurring across the country to date, including information on changing relationships between the main conflict actors. The project tracks more than 5,000 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 areas controlled by opposition forces, and areas where control is contested the proportion is significantly lower, yet still makes up 13% of all killings. The proportion is lowest in areas controlled by Kurdish forces, and by Islamic State.

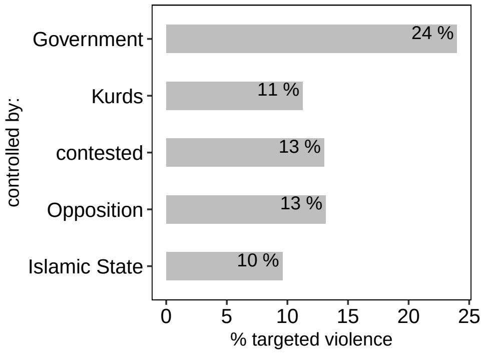

Figure 2. Percentage of violence that is targeted, by type of control.

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 lost territory in Aleppo, but gained ground in the northeastern 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 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

[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 1,000 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.

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	-2.486^{***}	-2.558^{***}	-1.419^{***}	-0.929	-0.417	-2.020	-4.273^{**}
	(0.209)	(0.269)	(0.407)	(0.550)	(0.366)	(1.289)	(1.359)
Internet access (3G)	0.268^{**}	0.294^{**}	0.268^{**}	0.267^{**}	0.301^{**}	0.366^{**}	1.003^{***}
	(0.094)	(0.090)	(0.085)	(0.087)	(0.115)	(0.119)	(0.133)
% Govt control							0.019^{***}
							(0.004)
Internet (3G) * % Govt control							-0.015^{***}
							(0.002)
Govt control	0.905^{**}	0.962^{***}	1.228^{***}	1.223^{***}	0.256	1.047^{**}	0.886^{**}
	(0.345)	(0.275)	(0.292)	(0.297)	(0.367)	(0.328)	(0.270)
IS control	13.995^{***}	14.838^{***}	14.385^{***}	-0.506^{*}	13.714^{***}	14.090^{***}	-0.831^{**}
	(1.178)	(1.188)	(1.176)	(0.241)	(1.167)	(1.167)	(0.257)
Kurd control	0.159	-0.472	-0.649	-2.263	-0.615	-0.149	-0.713
	(0.810)	(1.166)	(1.103)	(1.350)	(1.079)	(1.131)	(0.485)
Opp control	1.110^{***}	1.238^{***}	0.847^{**}	0.867^{**}	-0.669^{*}	-0.212	-0.173
	(0.316)	(0.348)	(0.328)	(0.333)	(0.304)	(0.370)	(0.176)
Internet (3G) * Govt control	-0.214	-0.249^{*}	-0.354^{**}	-0.345^{**}	-0.147	-0.414^{***}	
	(0.136)	(0.115)	(0.121)	(0.123)	(0.140)	(0.124)	
Internet (3G) * IS control	-14.069^{***}	-15.012^{***}	-14.888^{***}		-14.851^{***}	-14.800^{***}	
	(1.095)	(1.111)	(1.104)		(1.104)	(1.102)	
Internet (3G) * Kurd control	-0.132	0.330	0.135	1.686	-0.023	-0.183	
	(0.666)	(0.968)	(0.912)	(1.094)	(0.894)	(0.870)	
Internet (3G) * Opp. control	-0.609^{***}	-0.762^{***}	-0.601^{***}	-0.620^{***}	0.301	0.248	
	(0.165)	(0.194)	(0.179)	(0.181)	(0.160)	(0.197)	
# Killings (log)			-0.196^{***}	-0.194^{***}	-0.300^{***}	-0.343^{***}	-0.528^{***}
			(0.054)	(0.055)	(0.051)	(0.072)	(0.077)
Govt gains				0.778^{*}			
				(0.375)			
Govt losses				0.620			
				(0.449)			
Christian					0.084	0.366^{**}	0.444^{***}
					(0.123)	(0.124)	(0.118)
Alawi					1.505^{**}	-1.268^{***}	-0.893^{***}
					(0.562)	(0.195)	(0.201)
Druze					-0.535^{*}	-0.214	0.261
					(0.209)	(0.213)	(0.225)
Kurd					-0.597^{**}	-0.503	-0.617^{*}
					(0.210)	(0.267)	(0.248)
Internet (3G) * Alawi					-0.969^{***}		
					(0.178)		
Pop (log)						0.220	0.504^{**}
						(0.177)	(0.187)
Unempl. (%)						-0.015	-0.002
						(0.013)	(0.013)
Temporal FEs		✓	✓	✓	✓	✓	✓
AIC	11310.335	9255.292	9097.176	8910.211	7256.724	7450.581	6922.218
BIC	11355.012	9501.015	9347.367	9159.171	7529.253	7727.578	7190.280
Log Likelihood	−5645.168	−4572.646	−4492.588	−4399.106	−3567.362	−3663.291	−3401.109
Deviance	9032.435	6887.391	6727.276	6594.656	4876.823	5068.681	4544.318
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 neither 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. 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.

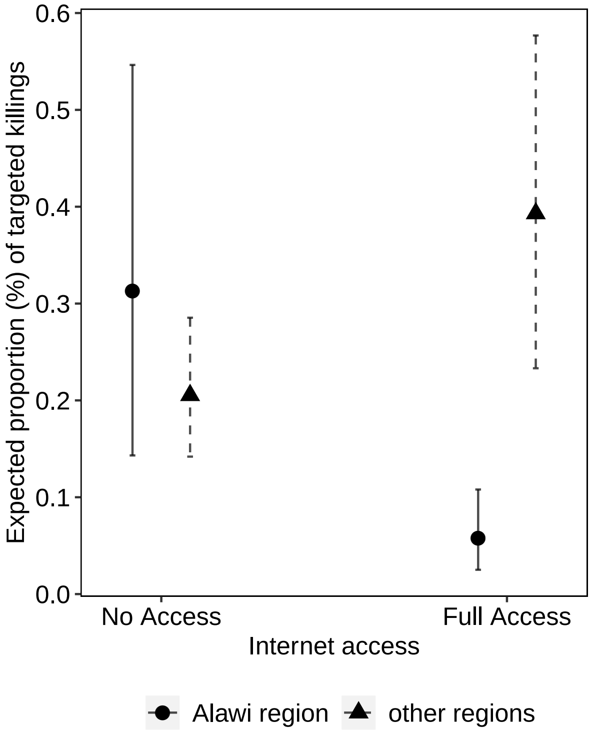

Figure 3. Expected proportion of targeted killings, given Internet accessibility and whether a region is inhabited by the Alawi minority.

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, but not 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 by 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.

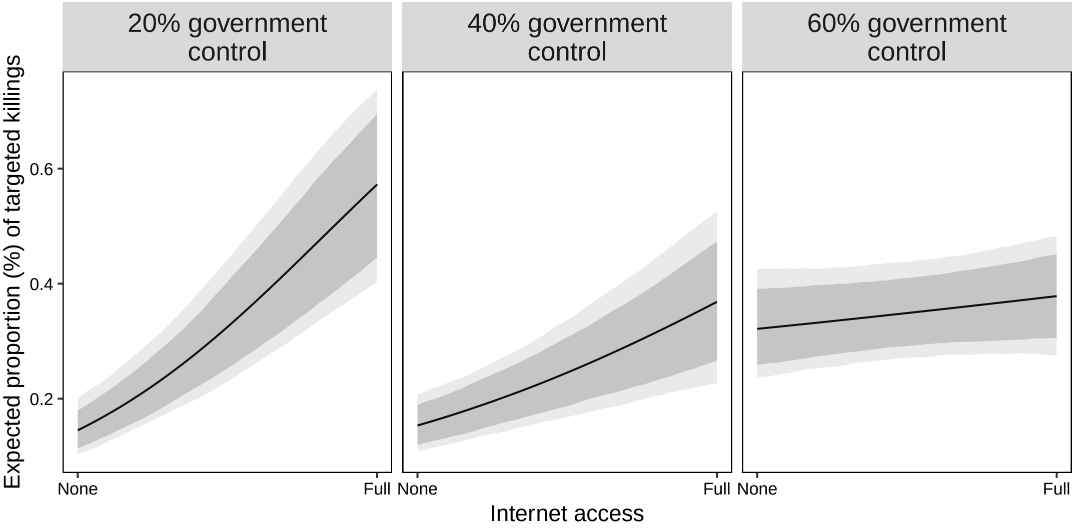

Figure 4. Expected proportion (83% and 95% confidence intervals) of targeted killings, given Internet accessibility and different levels of government control.

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, in 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 one 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 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 the 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 who show 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 underresearched. 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-Hussien, Obada. 2017. "Internet is back in Raqqa countryside areas." *Northern Syria Observer* . (accessed 2019-01-15).
URL: *https://www.nso-sy.com/Details/752/Internet-is-back-in-Raqqa-countryside-areas/en*

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 University 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*

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*

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)5490*

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.