Information and Communication Technologies and the Dynamics of Civil Conflict

Mehmet Erdem Arslan

A thesis submitted for the degree of

Doctor of Philosophy

Department of Government

University of Essex

August 2023

Acknowledgements

I wish to express my gratitude to the Ministry of Education and the Gendarmerie General Command of the Republic of Türkiye for their unwavering support and generous funding throughout my doctoral journey. My supervisor, Kristian Gleditsch, has been an exceptional source of guidance and inspiration. His continuous support and excellent academic mentorship have played a pivotal role in shaping my research and nurturing my intellectual growth during my time at the University of Essex. I am also deeply grateful to my co-supervisors, Howard Liu and Prabin Khadka, as well as my board member, Han Dorussen, for their insightful comments and profound advice, which have significantly enriched my work. The Department of Government and the IR/Conflict research division at the University of Essex have created a stimulating and encouraging environment for my academic and professional development. Throughout these three years, numerous individuals have generously provided invaluable feedback on this project. While it is impossible to list everyone here, I am sincerely indebted to Sara Polo, Miranda Simon, Brian Phillips, Ximena Velasco Guachalla, Andreas Juon, Michael Rubin, Tolga Sınmazdemir, David Weyrauch, Blair Welsh, Lorenzo Crippa, Nelson Ruiz, Sergi Martinez, Neil Mitchell and the many others who participated in workshops and conferences I was lucky to be present. Lastly, my heartfelt thanks go out to all my dear friends at the University of Essex. Your companionship and support have made this journey not only easier but also enjoyable.

Abstract

This thesis explores the impacts of information and communication technologies (ICTs) on the dynamics of civil conflict, through three journal-style articles that are interrelated but examine different research questions. The first article examines the rationale behind violent attacks on telecommunication infrastructure by non-state actors during civil wars. Building on existing literature concerning rebel targeting, it posits that rebel groups engage in such targeting when they perceive a significant risk to their survival. This risk becomes more pronounced as rebels confront military forces with enhanced capabilities for detecting and targeting militants. Additionally, the article sheds light on the specific tendencies driven by the ideology of the group concerning target selection. The second article investigates the potential use of modern communication technologies by rebel groups and their impact on organisational effectiveness in ongoing conflicts, focusing on the third-generation mobile network in Afghanistan as a case. It contends that the adoption of modern communication technologies can yield improvements in areas where rebels already utilise telecommunications to some degree, including in-group monitoring, indoctrination and propaganda, diffusion of knowledge, real-time coordination, and intelligence gathering. The third article explores how state control over ICT infrastructure can facilitate digital surveillance and hinder militant mobilisation, prolonging the escalation of armed conflict. By linking the control of companies to the ownership structure, it offers a comprehensive overview of how states can exploit their control over ICT infrastructure to detect potential uprisings and preemptively respond to armed challengers. The findings of this thesis underscore the paramount significance of information in civil conflicts, particularly in scenarios where significant disparities in capabilities exist between opposing forces. Moreover, the thesis enhances our understanding of the interplay between information and communication technologies and conflict dynamics, illuminating how conflict actors strategically adapt their approaches in response to the opportunities and challenges presented by communication technologies.

Contents

Acknowledgements **iii**

Abstract **v**

1 Introduction **1**

1.1 Communication Technologies and Protest 3

1.2 Communication Technologies and Civil Conflict 4

1.3 Motivation 6

1.4 Key Assumptions and Concepts 8

1.5 Overview of the Chapters 10

2 Targeting Telecommunications: Why Do Rebel Groups Target Information and Communication Technology Infrastructure? **15**

2.1 Introduction 16

2.2 The Logic of Targeting Telecommunications 20

2.2.1 Targeting to Survive 22

2.2.2 Targeting to Defend the Echo-chamber 25

2.3 Data 28

2.3.1 Dependent variable 28

2.3.2 Independent variables 30

2.3.3 Confounders 31

2.4 Analysis 33
2.5 Conclusion 39
2.A Summary statistics and the correlation matrix of independent variables . . . 41
2.B Additional information on the data 42
2.C Data on the ideological orientations of the rebel groups 44
2.D Robustness checks 48
2.D.1 Improvements in Predictive Power: ROC and PR Curves 48
2.D.2 Replications with different types of telecommunication infrastructure 49
2.D.3 Replications with different subsets of time periods 50
2.D.4 Interacting ideologies with government censorship and media bias indicators from V-dem 50
2.D.5 Fixed effects models 52
2.D.6 Other robustness checks 53
2.D.7 Replications with different outcomes and alternative explanations . . 54
2.D.8 Alternative measurements of the dependent variable in terms of coding uncertainty 56
2.D.9 Sensitivity tests 57

3 Did 3G Make Afghan Insurgents Fight More Effectively? A Disaggregated Study 61

3.1 Introduction 62
3.2 A Brief Overview of the Literature 64
3.3 Modern Communication Technologies in Civil War 66
3.4 War and Telecommunications in Afghanistan 73
3.5 Data and Research Design 76
3.5.1 Dependent Variable 76
3.5.2 Independent Variable 79
3.5.3 Research Design 80

3.6 Results . . . 84
3.6.1 Matched Wake Analysis . . . 84
3.6.2 Spatial Regression . . . 86
3.6.3 Placebo Tests . . . 89
3.6.4 Additional Robustness Checks . . . 90
3.6.5 Limitations . . . 92
3.7 Conclusion . . . 93
3.A Detailed results for H2 (IED attacks) . . . 95
3.B Regression Results using GTD events . . . 96
3.C Test of Potential Reporting Bias in GTD Between 2G and 3G Network Coverage 97
3.D Detailed Results of Placebo Tests . . . 99
3.E Effects of 3G on Attacks by Government Forces . . . 103
3.F Regression results with the alternative definition of multiple coordinated attacks 105
3.G Results including covariates in DD regression . . . 106
3.H Results excluding Kabul City . . . 108
3.I Map of secondary level administrative units (Wuleswali) . . . 108

4 State Control Over Telecommunications, Surveillance, and Militant Mobilisation 109

4.1 Introduction . . . 110
4.2 Overview of the literature and motivation . . . 112
4.3 Surveillance against mobilisation . . . 116
4.4 Data . . . 124
4.4.1 Dependent variable . . . 124
4.4.2 Independent variable . . . 125
4.4.3 Confounders . . . 127
4.4.4 Modelling Mobilisation . . . 130
4.5 Analysis . . . 131

4.6 Discussion and Conclusion 137
4.A Correlation matrix of independent variables 140
4.B Lagged values of the independent variables 141
4.C Domestic shares of ISPs as the independent variable 142
4.D Country-level analysis 143

5 Conclusion **147**

5.1 Summary of the findings 147
5.2 Limitations 149
5.3 Policy implications 151
5.4 Directions for future research 152

Bibliography **155**

List of Figures

2.1 Number of attacks to telecommunication infrastructure over time 29

2.2 Histogram of military expenditures per military personnel (country-year observations) 30

2.3 Numbers of rebel groups and ideologies over time 31

2.4 Military expenditures per military personnel (log scale) and the number of attacks to telecommunications 34

2.5 Predicted probabilities of targeting telecommunications 37

2.6 ROC and PR curves 48

2.7 Sensitivity test for *military expenditures per military personnel* 58

2.8 Sensitivity test for *Marxist-socialist ideology* 59

3.1 Evolution of Mobile Network Coverage in Afghanistan 77

3.2 Empirical results of matched wake analysis 87

3.3 Placebo tests for *H1* and *H2* 91

3.4 Testing potential reporting bias 98

3.5 Effects of 3G Network on the Attacks by Government Forces 103

3.6 Results of matched wake analysis (with covariates included in DD regression) 106

3.7 Results of matched wake analysis (excluding Kabul City) 108

3.8 Map of 2nd Level Administrative Areas 108

4.1 Armed group mobilisation 125

4.2 Density plot of state shares of ISP companies by country-years (2000-2019) . 127
4.3 Survival curves for varying levels of state share of ISPs (Model 1, full sample) 132
4.4 Survival curves for varying levels of state share of ISPs, grouped by minumum, maximum and quartile values of mobile phone subscriptions per 100 people (Model 2, full sample) 133
4.5 Estimated coefficients for the main independent variable using samples with increasing thresholds for battle-deaths 136

List of Tables

2.1 Cost and benefits of telecommunication infrastructure in an ongoing conflict 21

2.2 Number of conflict-dyad years with at least one attack to telecommunications infrastructure 34

2.3 Regressions on targeting telecommunications 36

2.4 Summary statistics 41

2.5 Correlation matrix 41

2.6 Share of ideology categories 44

2.7 Logistic regressions on attacks to different types of telecommunication infrastructure 49

2.8 Regressions on targeting telecommunications with subsets of different time periods 50

2.9 Interacting ideologies with censorship and media bias indicators 51

2.10 Fixed effects models 52

2.11 Robustness checks 53

2.12 Replications with different outcomes and alternative explanations 55

2.13 Regressions with alternative measurements of the DV (Different uncertainty levels in TAC project) 57

3.1 Insurgent use of ICT and their implications 70

3.2 Overview of the Matched Wake Analysis Results 88

3.3 Regressions on multiple coordinated attacks 89

3.4 Overview of the Matched Wake Analysis Results with IED Attacks as the Dependent Variable 95
3.5 Spatial and TWFE Regression Results with GTD data 96
3.6 Overview of the Placebo Test for *H1*: Installations of 3G Towers 3 Months Before the Original Date (Matched Wake Analysis) 99
3.7 Overview of the Placebo Test for *H1*: Installations of 3G Towers 6 Months Before the Original Date (Matched Wake Analysis) 100
3.8 Overview of the Placebo Test for *H2*: Installations of 3G Towers 3 Months Before the Original Date (Matched Wake Analysis) 101
3.9 Overview of the Placebo Test for *H2*: Installations of 3G Towers 6 Months Before the Original Date (Matched Wake Analysis) 102
3.10 Overview of the Results with Government Attacks as the Dependent Variable (Matched Wake Analysis) 104
3.11 Regression results with the alternative definition of multiple coordinated attacks 105
3.12 Overview of the Matched Wake Analysis Results (with covariates included in DD regression) 107

4.1 Summary statistics 129
4.2 Cox proportional hazard models 134
4.3 Correlation matrix 140
4.4 Replication of Table 4.2 with lagged values (1 year) of independent variables 141
4.5 Replication of Table 4.2 with domestic shares of ISPs as independent variable 142
4.6 Country-level analysis: Logistic regressions on civil conflict onset 145

Chapter 1

Introduction

This thesis explores the impacts of communication technologies on the dynamics of civil conflict, through three journal-style articles that are interrelated but examine different research questions. I aim to advance our understanding on the actions and strategies of the warring parties in response to the opportunities and risks presented by information and communication technologies (ICTs). In each substantive chapter, I focus on a specific aspect of this overarching theme. First, I analyse the logic behind violent attacks to telecommunication infrastructure by non-state actors during civil wars. Second, I explore the potential use of modern communication technologies by rebel groups and how they can relate to organisational effectiveness in ongoing conflicts, focusing on the third-generation mobile network in Afghanistan as a case. Third, I investigate how state control over telecommunication infrastructure can hinder militant mobilisation and prolong the escalation of armed conflict. The findings underscore the importance of control and access to information in civil wars and suggest that communication technologies matter.

In recent decades, we have witnessed an unprecedented pace in the evolution of information and communication technologies. The increased capacity for information exchange and reduced costs have made people around the world more connected than ever. As of 2022, it is estimated that two-thirds of the global population have access to the Internet,

three-quarters own a mobile phone, and 95% are covered by at least a 3G mobile network (ITU, no date). The number of social media users has reached 4.9 billion (Wong, 2023), and in 2022 alone, 1.21 billion smartphones were sold (IDC, 2023). These technologies have become integral to our daily routines, and societies are increasingly relying on them in trade, education, public health, and various other sectors. The swift and extensive changes brought about by these advancements can have profound impacts on social outcomes, and scholars are trying to comprehend their short- and long-term implications for societies.

This line of enquiry is not merely an intellectual pursuit but also holds significant relevance for policy challenges. However, keeping up with technological advancements poses a challenge for policymakers and social scientists alike. Understanding the impacts and implementing effective regulations can often lag behind the rapid introduction and proliferation of such technologies. Ideally, the objective of policy-making is to identify and mitigate potential negative effects while maximising positive outcomes. Although decisions on categorising outcomes as negative or positive can be subjective and constantly debated, there is consensus on certain aspects, such as the positive relationship between economic growth and ICT use, attributed to learning, technology diffusion, innovation, improved decision-making quality, and reduction in costs (Aker and Mbiti, 2010; Awad and Albaity, 2022; Vu, Hanafizadeh and Bohlin, 2020; Vu, 2011).

Communication technologies are primarily used to connect users and facilitate the flow of information between them. New technologies exponentially increased the richness of content and the speed of dissemination of information, while decreasing the costs of accessing and exchanging information. This seemingly straightforward observation has a particular implication among many: Communication technologies can alleviate collective action problems. Well-connected societies with high levels of information flows are expected to coordinate better. For example, decentralised communication platforms, such as social media, created a virtual public space where citizens can express themselves to an audience much larger than their offline circle. If collective action and coordination problems are overcome, citizens can

raise their voices more effectively and increase their odds of leading to a change toward their will.

1.1 Communication Technologies and Protest

Social movements such as the Arab Spring and the Occupy movement have generated a great deal of interest and have provided support for the view that ICT can benefit collective action. Scholars and activists interpreted these salient events as indications of the potential effects that ICTs can have on protests and contentious politics. A fruitful debate started, and a large body of literature examined the role of modern ICTs in protests and democratic regime change, some referring to it as 'liberation technology' (Diamond, 2010). Tufekci and Wilson (2012) documented that social media users were more likely to participate in the first days of the Tahrir Square protests in Egypt. Edmond (2013) argued that decentralised information technologies can make regimes easier to overthrow compared to centralised media, such as radio or newspapers. Christensen and Garfias (2018) found that mobile phone coverage increases the probability of protests. Weidmann and Rød (2019) differentiated between the onset and the continuation of protests and argued that in autocracies internet access can strengthen ongoing dissent. Manacorda and Tesei (2020) empirically tested the relationship between mobile phone coverage and protests and found that mobile phones can contribute to mass mobilisation in Africa during economic decline.

The recent literature has also recognised the flip side of the coin: the potential use of ICTs by the state as a tool for repression and control (Morozov, 2011) Digital surveillance, for instance, can address the information problem faced by authoritarian governments by revealing the true preferences of citizens regarding the regime (Xu, 2021). Furthermore, governments may resort to network shutdowns to disrupt the coordination of protesters during periods of dissent (Howard, Agarwal and Hussain, 2011). Internet shutdowns during protests in Iran and the use of digital surveillance by the Chinese government in Xinjiang

have exemplified the potential implications of state control of telecommunications.

1.2 Communication Technologies and Civil Conflict

The theoretical arguments proposed within the literature on ICTs and protest set a guideline for studies of violent conflict, as the former is more developed partly due to the availability and quality of the data. Existing theories, such as collective action, free-riding, or information asymmetries, are adapted and tested to understand the changes that ICTs can bring about in conflict settings (Gohdes, 2018, p. 93). Central questions in this domain revolve around whether and how ICTs prove effective in mobilisation at the onset of conflict, and in coordination during the conflict. The expected implications are similar for both the onset and dynamics of violent conflict. Does ICT lower the barriers for collective action and make it easier to organise a rebellion by facilitating more effective propaganda, recruitment, within group coordination, and monitoring? Conversely, does it diminish the opposition's ability to challenge the state by providing states with an asymmetric advantage in controlling the information domain? Does it enhance safety for the population in sharing information about insurgents and providing more accurate intelligence about insurgent activity?

A growing body of literature has been seeking answers to these questions. Pierskalla and Hollenbach (2013) find that cell phone coverage increased the probability of violent conflict in Africa. Bailard (2015) examines ethnic groups and draws similar conclusions, proposing opportunities and motivations for conflict as explanations. On the other hand, Weidmann (2016) shows that cell phone coverage can increase the probability of a violent event being reported in the news media and therefore induce bias in studies using media-based conflict event data. Shapiro and Weidmann (2015) find that increased cell phone coverage in Iraq is associated with reduced insurgent violence, probably due to increased information flow from the population to the government. Such contradictory conclusions suggest that the effect of ICTs on violent conflict may be context-dependent, particularly concerning the extent to

which conflict actors can leverage the advantages of ICTs. Shapiro and Siegel (2015) analyse this by assessing relative gains to conflict actors using a formal model. Proposing a theory in line with this approach and applying it to the context of terrorism, Mahmood and Jetter (2020) find a non-linear relationship in which terrorist events first increase as the amount of information flow increases in a country and then decrease with the further increase in information flow.

States also have the ability to leverage their control over the ICT infrastructure and mass media during conflicts. Gohdes (2020) argues that states can provide internet access selectively depending on their intention to gain intelligence or undermine insurgent activity and coordination, and finds that in Syrian conflict, a high level of internet accessibility is associated with an increase in selective state violence, whereas areas with limited access are more likely to experience indiscriminate state violence. In a study of cell phone shutdowns in Pakistan, Mustafa (2023) finds that while the frequency of terrorist attacks tends to decrease in the days of shutdowns, it increases after the shutdowns end. Similarly to modern ICT, the effects of mass media on conflict are likely to vary across different contexts. Although radio broadcasts have been shown to have an effect on participation in killings in Rwandan genocide (Yanagizawa-Drott, 2014), Warren (2014) shows that mass media infrastructure is associated with a significantly lower probability of conflict in a study of 177 countries covering the period between 1945 and 1999,

Recent studies also acknowledge that different types of ICT may have different implications. Social media, for example, is gaining increasing attention, both in terms of its effects on conflict and its promising potential as an alternative data source, especially in places where access is limited (Unver, 2018). It has changed the direction of mass communication, democratised it by decentralising the communication environment and ending the elite monopoly on creating content and narrative (Zeitzoff, 2017). Warren (2015) shows that higher levels of social media penetration are associated with an increase in violence in a subset of African states. Zeitzoff (2018) finds that public support in social media can shift

conflict intensity, suggesting social media's effect on the micro-dynamics of conflict. While political elites, government agencies, and rebel groups are increasingly using social media to communicate with the masses, social media platforms themselves have also become actors, with their policies and algorithms having significant implications that are yet to be explored (Zeitzoff, 2017).

1.3 Motivation

To develop a more comprehensive understanding of the relationship between ICTs and civil conflict, several gaps need to be addressed. First, while rebel groups are expected to benefit from available technologies, the telecommunication infrastructure is often directly targeted by rebel groups in civil wars. It often goes unnoticed that the use of communication technologies for within-group communication in rebel organisations resembles 'signal communications' in conventional armies. The importance of signal communications in interstate wars is long-established, and communication assets are often targets of high-priority for each side, while interception of the enemy communications is also desired. If ICTs are providing advantages for any side in 'small wars,' we should also anticipate the targeting of ICT infrastructure, as actors would have incentives to destroy them when they perceive them as detrimental. However, limited information is available regarding the extent and systematic nature of such targeting, as well as the rationale behind rebel groups' decisions to target telecommunications. Considering the asymmetric nature of intrastate wars, states can opt for network shutdowns instead of attacking the infrastructure, since they often control the infrastructure.

Second, the debate regarding the effects of ICTs on collective action in violent conflict remains unresolved. This is particularly pertinent in the case of cell phone technology, which is widely used, easily accessible, and increasingly capable of facilitating internet access. Previous studies have empirically examined the presence of mobile networks versus their absence, raising concerns about endogeneity and reporting bias. However, there is now meaningful

variation in this technology, with opportunities to gain a better understanding of the modern ICTs-collective action nexus. Since the introduction of the third generation (3G) mobile network, cell phones have evolved to a medium that allows the transmission and reception of voice and video messages, as well as internet browsing, thereby approaching the level of face-to-face communication. Such technological advancements may have implications that have yet to be explored, and they can also be leveraged to test existing theories more robustly. Specifically, examining the impact of 3G on violence in comparison to the older 2G network can provide compelling insights about the link between communication technologies and collective action.

Third, it is often assumed that states have complete and constant control over telecommunication infrastructure, including the ability to intercept all communications or completely shut down networks. However, this assumption is unlikely to hold. The extent to which states can leverage control over infrastructure may depend on (i) the ownership of telecommunication companies, (ii) the degree of compliance of telecommunication companies not owned and controlled by the state, and (iii) the access to advanced surveillance tools, which all vary across countries and over time. While nationalisation or privatisation of the telecommunications companies suggest changes on the extent of control, accessibility to the advanced surveillance products depends on economic power and bilateral relations, as very few states and companies offer them. ICTs have been argued to facilitate new and effective means of state surveillance, and governments can also utilise their control over ICT infrastructure to undermine rebel collective action through network shutdowns. However, the implications of variation in state control of telecommunications for armed mobilisation and conflict have not yet been explored. In particular, if state control over ICT infrastructure enables digital surveillance, we should observe militant mobilisation hampered as a consequence.

Addressing these shortcomings and gaining a better understanding of the impacts of communication technologies on the dynamics of civil conflict is important not only as a scholarly contribution, but also as a policy. Modern communication technologies are viewed

as drivers of economic development (e.g., Vu, Hanafizadeh and Bohlin, 2020), and economic decline and poverty are often associated with dissent and conflict (e.g., Bazzi and Blattman, 2014; Buhaug et al., 2021; Dube and Vargas, 2013; Malone, 2022a), which in some cases led to policies that support the expansion of network infrastructure to reduce opportunities for violence. However, our understanding of the strategic implications for conflict actors with respect to access to such technologies remains unclear. This is also relevant for states, as they increasingly employ new and innovative technologies for surveillance (DeSombre, Gjesvik and Willers, 2021; Feldstein, 2019; Privacy International, 2016). As we try to comprehend the impact of existing technologies, new ones continue to emerge, potentially altering the current understanding and necessitating a re-evaluation of their implications for societies, including violent conflict. For instance, global access to the Internet via satellites (e.g. Starlink) with little or no infrastructure on the ground can eradicate state control over telecommunication infrastructure. By gaining a better understanding of the implications of today's technologies, we can be better equipped to assess the potential impacts of future technologies.

1.4 Key Assumptions and Concepts

This thesis contributes to the existing academic literature by addressing the aforementioned gaps through three interconnected papers that examine the relationship between ICTs and conflict dynamics. Before providing a summary of the chapters, it is important to briefly describe the underlying paradigm guiding my approach and provide definitions of key concepts. I assume that conflict actors act rationally, assess the perceived benefits and costs of their actions, and pursue activities that they consider benefits outweigh costs. In the context of intrastate war, the primary goal of actors is to ensure their survival and avoid the ultimate cost. Although fighting a war is a costly and inefficient action compared to peace, failures in bargaining can lead to the outbreak of wars (Fearon, 1995). Once belligerents are involved in violent conflict, their aim is to minimise costs imposed upon themselves while maximising

the costs imposed upon their adversaries. Consequently, actors seek opportunities to impose such costs, and they actively seek information about their adversaries that might aid in this endeavour.

Throughout the chapters, ICT or telecommunications refers to various types of technologies that facilitate the flow of information over distances. This can take the form of unidirectional communication, where information flows from a central node to the masses, such as radio, television, or the internet. It can also involve bidirectional communication between individuals, such as fixed or mobile telephone lines, radio communications, or social media platforms. Accordingly, telecommunication (or ICT) infrastructure refers to facilities for transmission of information such as cell phone towers, television transmitters, radio stations, as well as private or public bodies providing and maintaining telecommunication services. In the context of intrastate conflict, this flow of information serves to connect the warring parties and civilians with one another while also facilitating communication within organisations.

Adapting the definition of the Uppsala Conflict Data Program (UCDP), I define intrastate conflict as 'a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, between a government of a state and a non-governmental party, results in at least 25 battle-related deaths in one calendar year' (Pettersson, 2020). While UCDP categorises intrastate armed conflicts with more than 1000 battle deaths as 'wars,' I use intrastate conflict, civil conflict, and civil wars interchangeably throughout the text. When referring to the non-governmental party in intrastate armed conflict, I use rebel group and insurgent group interchangeably, and similarly use rebels, insurgents, and militants when referring to the combatants in those groups.

1.5 Overview of the Chapters

In the next chapter, I investigate under which conditions rebel groups target telecommunication infrastructure in civil conflicts. I demonstrate that some rebel groups systematically target telecommunications while others do not, and I argue that these choices reflect deliberate decisions based on perceived costs and benefits. These decisions are often shaped by the relative weakness of the rebel groups compared to the government and the dynamics of the battlefield. When faced with a government possessing technologically advanced military capabilities, rebels are more inclined to target telecommunication infrastructure to avoid detection and being targeted by government forces. However, there is a threshold beyond which a further increase in the opponent's technological capabilities may prompt rebels to employ alternative preventive measures instead of targeting telecommunications. Moreover, Marxist-socialist or religious groups are anticipated to be more likely to target telecommunications in order to maintain an 'echo-chamber' within their constituency, facilitating indoctrination and propaganda. These ideologies seek to establish new norms, rules, and societal reorganisation spanning from social relations to economic activities. Given the fundamental transformation advocated by these ideologies, the dissemination of propaganda and outreach directed at their constituency becomes crucial, along with the hindrance of anti-rebel propaganda. Consequently, the motivation arises to create new means of propaganda, gain control over existing channels and facilities, and destroy those that cannot be controlled.

I test these arguments with an analysis of rebel groups coded in the UCDP Dyadic dataset (Pettersson and Öberg, 2020; Themnér and Wallensteen, 2014), using information on attacks on telecommunications from the Global Terrorism Database (GTD) (START, 2021). I use the recent Terrorism in Armed Conflict (TAC) data project to combine the two sources (Fortna, Lotito and Rubin, 2022). In analysis of 372 rebel groups for the period between 1970-2013, the findings reveal an inverted U-shaped curvilinear relationship between the technological sophistication of the government's military, measured by military expenditures per military

personnel, and the probability of targeting telecommunications. Rebel groups facing military forces with moderate levels of technological sophistication are found to have the highest likelihood of targeting telecommunications. Moreover, groups advocating Marxist-socialist or ethno-religious ideologies exhibit a greater propensity to conduct attacks on telecommunications compared to groups with other ideologies.

In the third chapter, I revisit the modern ICTs–collective action nexus. While previous studies have produced contradictory findings regarding the impact of communication technologies on civil conflict, it is essential to acknowledge that these technologies have continued to evolve, bringing about significant changes in the nature of telecommunication itself. The subsequent generations of technologies offer much more advanced capabilities, suggesting that their impact on conflict dynamics should be more pronounced compared to earlier generations. This is particularly notable when transitioning from 2G to 3G networks, as the introduction of the 3G network fundamentally transformed mobile communications, moving closer to face-to-face interaction.

I argue that the introduction of the 3G network in areas already covered by 2G networks facilitated improved communication among insurgents, enhancing their military operations and consequently leading to an escalation of violence during high-intensity episodes of civil war. This argument is tested with a disaggregated study of the war in Afghanistan, using the Open Cell ID dataset for information on network coverage and the Significant Activities (SIGACTs) dataset of the US Department of Defense for information on violent events (Shaver and Wright, 2016). Using matched wake analysis to address the modifiable areal unit problem and mitigate selection bias (Schutte and Donnay, 2014), the results demonstrate a positive relationship between the introduction of the 3G network and insurgent attacks in various forms. These findings are further validated through spatial regressions utilising the Global Terrorism Database (GTD) as an alternative source of information on violent events.

In chapter four, I turn to the state as the other principal actor in intrastate wars and investigate the varying degrees of state control over telecommunication infrastructure. While

rebel groups utilise ICTs for purposes such as propaganda and coordination, states can leverage their control over the network infrastructure for intelligence gathering and, at times, to disrupt rebel coordination by shutting down networks. However, existing theoretical accounts often assume that state control over infrastructure is total and constant, overlooking the variation in ownership and control of telecommunication infrastructure between and within states over time. My aim is to fill this gap by examining the relationship between states' ownership of telecommunication companies and armed mobilisation.

I argue that control over telecommunication infrastructure enables states to engage in surveillance efforts, effectively monitor dissent, and access critical information to selectively target militants before an armed group gains sufficient power to challenge the state and escalate into a civil conflict. I consider ownership to be the most evident indicator of control, measured by the states' shares of telecommunication companies (Freyburg and Garbe, 2018). Using datasets on armed group mobilisation (Malone, 2022b) and ownership of telecommunication companies (Freyburg, Garbe and Wavre, 2023), I test these arguments for armed groups in Africa for the period 2000-2012. The results indicate that an increase in the state's share of telecommunication companies is associated with a longer mobilisation duration for armed groups, thereby decreasing their likelihood of successful mobilisation.

I conclude in the last chapter with a review of the key findings and contributions, followed by a thorough discussion of the limitations of the study. Additionally, I delve into potential policy implications and end the chapter by providing recommendations for future research. In its entirety, this thesis significantly advances our understanding of the intricate relationship between ICTs and conflict, while also making noteworthy contributions to the existing literature on rebel group target selection, state capacity and repression. Throughout the three substantive chapters, the strategic importance of information in intrastate conflicts becomes increasingly evident. The improved coordination resulting from information processing and communication within organisations can play an important role in shaping strategies of the belligerents. Moreover, the possession or pursuit of access to information and intelligence can

influence outcomes for the warring parties, creating incentives, in turn, to deny opponents from acquiring information.

Chapter 2

Targeting Telecommunications: Why Do Rebel Groups Target Information and Communication Technology Infrastructure?

Abstract

Although there has been much interest in how communication technology can shape conflict, the deliberate targeting of the telecommunication infrastructure by rebel groups has been largely overlooked. This chapter demonstrates that while some rebel groups are systematically targeting telecommunications, others do not. It is argued that this reflects deliberate choices, and rebel groups adapt strategies based on cost-benefit analysis. Given the aim of avoiding detection and being targeted, rebels are more likely to target the telecommunication infrastructure when faced with a government with a technologically sophisticated military. However, a further increase in the opponent's technological capabilities beyond a certain tipping point may compel rebels to employ preventive measures other than targeting telecommunications. Marxist-socialist or religious groups are also expected to be more likely to target telecommunications to try to maintain an echo chamber in their constituency to facilitate indoctrination and propaganda. These expectations are evaluated in an analysis of all rebel groups for the period 1970-2013. The results show a non-linear relationship between rebel targeting of telecommunication infrastructure and technological capabilities of the government forces, while Marxist-socialist and ethno-religious groups are more likely to target telecommunications compared to other groups.

2.1 Introduction

The last two decades have witnessed a rapid and revolutionary change in technology and media of communication, with profound yet complex and diverse effects on societies. The introduction of internet, cell phones, and social media has received considerable attention, and there is much debate among scholars about the long-term effects of these technologies. Salient events such as the Arab Spring or the Occupy Movement triggered the growth of the literature on information and communication technologies (ICT) and political protests (e.g. Christensen and Garfias, 2018; Little, 2016; Rød and Weidmann, 2015; Tufekci and Wilson, 2012), and many studies examine whether ICTs can facilitate collective action in armed conflict (e.g. Bailard, 2015; Mahmood and Jetter, 2020; Pierskalla and Hollenbach, 2013; Shapiro and Siegel, 2015; Shapiro and Weidmann, 2015; Warren, 2015). While there has been much interest in the relationship between ICT and political protest, repression, and armed conflict, violence directed at ICT infrastructure and companies has received less attention. According to the Global Terrorism Database (GTD), the proportion of attacks on the telecommunication infrastructure varies from zero to 30%, and even the most violent groups exhibit considerable variation.[1] For instance, ISIL and Houthi extremists (Ansar Allah) have no recorded attacks on the telecommunication infrastructure even though they are among the ten most violent groups in GTD. Therefore, targeting of telecommunications may not be a byproduct of violence in general, but rather a function of dynamics in a conflict.

Some rebel groups clearly target ICT, while others intend to exploit all that functioning ICT can offer. In Iraq, for example, insurgents pressured mobile network companies to build towers and 'guarantee safety to maintain their networks' (Blakely, 2005). In Afghanistan, the Taliban systematically attacked ICT (Shevory, 2016), demanded companies to switch off their cell phone towers throughout the day except for a few hours, and destroyed the cell phone towers of companies that do not obey their demands (Wesal, 2018). Violence can also

[1] I use 'ICT' and 'telecommunications' interchangeably.

victimise civilians associated with ICT companies, such as company officials (Hiiraan Online, 2018) or workers building a cell phone tower (Daily Balochistan Express, 2018). Although most attacks are standalone events, some of them are executed simultaneously throughout a country (The Himalayan Times, 2016). And in some cases, insurgents selectively target critical hubs and cut down mobile communications in an entire region (Boone, 2011). This study seeks to explore the drivers behind this phenomenon and understand the strategic choice of rebel groups to destroy or exploit the communication infrastructure.

ICT or telecommunications refers to various types of technologies that facilitate the flow of information over distances. This can be unidirectional, from a central node to the masses, such as radio, television, or the internet, or bidirectional between individuals such as fixed or mobile telephone lines, radio communications, or social media. Consequently, telecommunications infrastructure (or ICT) refers to facilities for transmission of information such as cell phone towers, television transmitters, radio stations, as well as private or public bodies providing and maintaining telecommunication services. In the context of intrastate conflict, this flow of information connects the warring parties and civilians with each other, while also facilitating communication within organisations.

The strategies rebel groups pursue are often reflected in their attack patterns and targets. A rich body of literature has focused on violence against civilians and often draws a dichotomous distinction between civilian and official targets (e.g., Asal et al., 2019; Balcells, 2010; De la Calle, 2017; Hultman, 2012; Humphreys and Weinstein, 2006; Kalyvas, 2006; Polo, 2020b). Recent work has stepped away from the civilian versus official target dichotomy to explore a wider range of target types. Polo and Gleditsch (2016) consider *hard* and *soft* targets, where the former includes non-lethal attacks targeting infrastructure among other target types. They show that different attack patterns of rebel groups are related to group resources, government responses, and group ideologies. Stanton (2013) differentiates between high- and low-casualty terrorism, defining low-casualty terrorism as the violence that has high costs for civilians, but not necessarily high casualties, such as attacks on infrastructure. We

still have limited understanding of why rebels chose specific targets and what these imply within an overall strategy.[2]

While the security risks to the telecommunication infrastructure in ongoing insurgencies have been highlighted before (e.g. Adebisi, Oyedeji and Azeez, 2015; Agubor, Chukwudebe and Nosiri, 2015), and preventive measures are discussed to protect critical infrastructure, including telecommunications (e.g. Bennett, 2018; Botha, 2021), the causes and logic of attacks on telecommunications in civil wars have received limited scholarly attention. However, there is a wealth of empirical work on the effects of 'modern' ICTs, such as cell phones, internet or social media, on conflict. Modern communication technologies allow for rapid dissemination of much more content, while decreasing the costs of acquiring information. Existing research suggests that while ICTs increased the probability of civil conflict (Bailard, 2015; Pierskalla and Hollenbach, 2013), they also reduced insurgent violence in some cases, possibly due to the increased flow of information from the population to the government (Shapiro and Weidmann, 2015). These studies suggest that the effect of ICT on conflict may depend on the context, particularly to the extent that parties can leverage the advantages of ICT (Shapiro and Siegel, 2015). States can exploit their control over ICT infrastructure to undermine insurgent coordination and communication (Gohdes, 2020; Mustafa, 2023). Telecommunication network coverage can also increase the probability of reporting events, thus inducing bias in studies relying on media-reported data (Weidmann, 2016).

Rebel groups' strategies and targets are mainly shaped by their relative weakness vis-à-vis the government and the dynamics of the battlefield. Their survival would be at risk if militants are effectively targeted at a higher rate than they recruit. Governments with higher technical and material capabilities, especially in surveillance and precision targeting, possess greater effectiveness in detecting and targeting rebels (Mir and Moore, 2019; Schwartz,

[2]The literature on sexual violence is another strand goes beyond the dichotomy of civilian versus official targets (e.g. Cohen and Nordås, 2014; Kreft, 2019; Wood, 2006). Other exceptions include studies investigating violence against peacekeepers (e.g. Fjelde, Hultman and Bromley, 2016; Salverda, 2013), schools (Asal, Phillips and Rethemeyer, 2022; Masullo and O'Connor, 2020), and journalists (Asal, Phillips and Rethemeyer, 2022; Gohdes and Carey, 2017).

Fuhrmann and Horowitz, 2022). In addition to military capabilities, governments need information on militant activities and whereabouts (Berman, Shapiro and Felter, 2011). This can be obtained from the local population and contribute to the government's victory, as it makes selective targeting possible (Lyall, Shiraito and Imai, 2015; Shaver and Shapiro, 2021). On the other hand, a rebel group would try to avoid this by disrupting the information flow to the government. They can target telecommunication infrastructure to sever the lines of communication between the government and the local population. This would reduce potential risks for the rebels and help them maintain their operations. However, in cases where targeting telecommunications is not sufficient to mitigate risks, rebels may instead resort to preventive measures to limit their exposure to the locals, by adopting a more covert structure and operating clandestinely. I posit that there exists a non-linear relationship between rebel targeting of telecommunications and the technological sophistication of the government forces. Specifically, the probability of targeting telecommunications increases as rebels confront a technically more advanced military, while it decreases beyond a certain tipping point when they face militaries placed at the higher end of the spectrum.

However, rebel groups also interact with the local populations, in particular with their constituency. The material and moral support of the locals, including recruitment, is the primary driver of the conflict and the main determinant of the strength of the rebel group. To mobilise popular support, rebels need an appealing cause presented in an ideology (Galula, 1964).[3] Some ideologies, in particular religious and Marxist-socialist ideologies, aim to construct new norms and rules, and reorganise the society from social relations to economic activities. Compared to the nationalist or other ideologies, advocacy for such fundamental transformation requires more propaganda and outreach directed at the constituency, along with the hindering of anti-rebel propaganda. This would motivate the creation of new means of propaganda, taking control of existing means and facilities, and destroying those that

[3]Following Gutiérrez-Sanín and Wood (2014, p. 214), I define ideology as 'a set of more or less systematic ideas that identify a constituency, the challenges the group confronts, the objectives to pursue on behalf of that group, and a (perhaps vague) program of action.'

cannot be controlled. To prevent government propaganda or the freedom press among local populations, rebels may target the telecommunication infrastructure to isolate the local population from government outreach.

I test these arguments with an analysis of rebel groups coded in the UCDP Dyadic dataset (Themnér and Wallensteen, 2014), using information on attacks on telecommunications from the Global Terrorism Database (GTD) (START, 2021). I use the recent Terrorism in Armed Conflict (TAC) data project to combine the two sources (Fortna, Lotito and Rubin, 2022). In analysis of 372 rebel groups for the period between 1970-2013, I find that technological sophistication of the government's military, measured by military expenditures per military personnel, exhibits an inverted U-shaped curvilinear relationship where the likelihood of targeting telecommunication is highest for the rebel groups facing militaries with medium levels of technological sophistication. Additionally, groups with Marxist-socialist or ethno-religious ideologies are more likely to attack telecommunications compared to groups with other ideologies. The findings are robust to a variety of alternative specifications and tests. In the following, I first elaborate on the proposed mechanisms and develop my hypotheses. I then detail the data and research design, followed by the presentation of the analysis and the findings. I conclude with a discussion of the implications and directions for future research.

2.2 The Logic of Targeting Telecommunications

I argue that the decision to attack telecommunications is driven by perceived costs and benefits, arising from the dynamic interactions between the conflict parties. In the context of an ongoing conflict, the potential benefits for one side constitute potential risks for the opponent. When the costs of ICT exceed benefits and rebels face a credible threat to survival, they are likely to target telecommunication infrastructure and instead rely on in-person communication with locals (such as using social connections or leaflets) and other available means for in-group communication (such as radios). Governments also weigh costs and benefits, but

in case of increasing costs, they can cut down telecommunications selectively in space and time rather than taking down the whole network, since they control ICT infrastructure. By disabling telecommunications, governments can deprive rebel groups of benefits, but this, in turn, may undermine their ability to target selectively (Gohdes, 2015; 2020).

Table 2.1 outlines the advantages and disadvantages of ICT for the parties to the conflict. I argue that costs associated with the leak of information about rebels to the government (i.e., human and signals intelligence) are higher for rebel groups that face technologically advanced militaries, which have means for both detecting and targeting militants effectively. As security forces become more technologically sophisticated, they would have more advanced tools to collect information, they would be able to act quicker upon the information to project force, and they would have more advanced systems to selectively target militants. These factors imply a greater risk to the survival of the rebel group. To alleviate this risk, rebels would target the lines of communication between locals and the government, in particular, the fixed and mobile phone lines and infrastructure. They may also limit the use of the telecommunication network within the militants, as a countermeasure for signals intelligence efforts of the government. For cases where these measures are not sufficient to decrease costs, rebels may go underground and limit the information available to the local population.

Government	Benefits	1. Signals intelligence from militant communications (SIGINT) 2. Information about militants from local population (HUMINT) 3. Propaganda of the government to the local population	Costs	Rebel group
	Costs	1. Within group communication and coordination for militants 2. Propaganda of the rebel group to the local population	Benefits	

Table 2.1: Cost and benefits of telecommunication infrastructure in an ongoing conflict

Propaganda efforts of the government, aiming to win local support while reducing support for rebels, constitute a greater risk to rebel groups that rely on indoctrination to gain local support and recruitment. Groups with ideological orientations that advocate for a fundamen-

tal social transformation, such as Marxist or religious groups, need to promote their ideology to the local population to mobilise resources. When government counter-propaganda can undermine support, rebel groups would have stronger incentives to target telecommunication infrastructure that facilitates government outreach to locals, such as radio or TV stations or internet network.

It is worth noting that rebel groups can limit the implementation of a targeting strategy to a certain geographic area. Having uncontested territorial control or safe haven over an area would create different incentives compared to contested territories with ongoing fighting between the rebel group and the government. In areas of uncontested control, means of mass communications (such as radio or TV stations) can be utilised to disseminate propaganda, and telecommunication network (such as cell phone towers or fixed landlines) can be a subject of service provision to a community where rebels do not perceive a risk of denunciation. Although groups with territory may not have incentives to attack the telecommunication infrastructure within their controlled territory, outside of their territory they would operate in a similar manner to groups without territory, for instance, operating covertly and using terrorist tactics more (Anders, 2020).

This assessment of costs and benefits pertains to the group leadership, and I assume that members of a rebel group act coherently. Ill-disciplined groups, which may use violence against civilians without the knowledge of the group leadership (Humphreys and Weinstein, 2006), are unlikely to violate this assumption, since attacking telecommunication infrastructure does not offer any immediate individual benefits to militants. I also assume that rebel groups have a political aim and a level of popular support, and the scope of the study excludes criminal violence and other groups without clear political motives.

2.2.1 Targeting to Survive

ICT infrastructure facilitates bidirectional flow of information between nodes and enables almost instant transmission, regardless of distance. This has impacts on intrastate conflicts, as

it facilitates interaction between conflict actors. For governments, connections to locals sustain the flow of information about rebels, which is critical for selective targeting of militants and undermining rebel organisations. For rebels, local people are a source of information about government activities, while they also need local connections to spread propaganda and recruit militants. For governments with relevant capabilities, another advantage of ICT is the intelligence collected through the use of telecommunications by rebels (Shapiro and Siegel, 2015).

Many intrastate wars are asymmetric, with governments much stronger than the insurgent group(s), and rarely fought by conventional means. Weaker insurgents adapt strategies to overcome their disadvantage, relying on guerrilla warfare such as hit-and-run tactics and using geographical features to hide. To overwhelm the insurgents, the government must first detect the presence of the rebels and then quickly deploy responses to the location. Detection of militant presence can be achieved via information from locals, or surveillance efforts such as detecting use of telecommunications by militants. Technically advanced militaries are better placed both to detect and to deploy responses, through means such as attack helicopters or armed drones. Improved government surveillance and precision targeting make it harder for rebels to survive, and to overcome this, they need to avoid detection in the first place.

To effectively challenge the government, rebel groups rely on garnering the support and loyalty of locals, either through voluntary consent or coercive means. Winning loyalty ensures that there is less willingness among the local population to share information about insurgent activities with the government, which possesses material superiority and is likely to overcome insurgents if it also enjoys an informational advantage. However, it is unlikely for rebels to entirely eliminate the risk of being denounced, and as the technological sophistication and capabilities of government forces increase, the hazard for rebels gets higher even with low probabilities of information leaks. This may create incentives for rebels to cut the lines of communication between the government and the local population, and stop the flow of information from locals to the government, by targeting telecommunication networks such as

phone lines or cell phone towers.

However, facing a very strong military in terms of technological capacity may compel rebels to adopt a more covert strategy, avoiding direct confrontation with government forces. In such cases, attacking telecommunication infrastructure may prove insufficient to reduce rebel losses to a sustainable level that allows them to maintain their violent activities. To further decrease the risk of being detected, rebels may choose to restrict their engagements with locals, thereby minimising the information available to local population. Under these conditions, targeting the telecommunication infrastructure may not yield clear benefits to the militants. Overall, I expect that increasing levels of technical advancement of the government military would make rebels more likely to target the telecommunication infrastructure to avoid detection and improve the chance of survival. However, very high levels of technological advancement beyond a certain tipping point may weaken this effect, since it would necessitate the adoption of a different strategy of insurgency by rebels.

The aim of preventing locals to inform on militants as well as preventing government surveillance is evident in several events. For example, before attacking the telecommunication infrastructure and companies in Nigeria, Boko Haram accused the telecommunication operators of 'providing the security personnel with information used to track their members' (Akwaja, 2012). In India, after a series of attacks on cell phone towers, a security officer claimed that the Maoists aimed to prevent locals from informing the police on their movements (The Times of India, 2015). In Afghanistan, a US official stressed that attacks by the Taliban on the telecommunication infrastructure aim to prevent locals from giving tips about insurgents and damaging counter-insurgency efforts (Boone, 2011). In an interview, a FARC commander stated that they ordered the destruction of a cell phone tower, with concerns over being detected by a potential information leak from militants or 'spies' (de Castro Leal et al., 2019, p. 7).

H1. A rebel group is more likely to target the telecommunication infrastructure as it faces a government with a technically more advanced military, while this probability declines beyond

a certain tipping point.

2.2.2 Targeting to Defend the Echo-chamber

To build and sustain an armed group of militants, rebels must recruit throughout the war, as they often seek to grow and need to replenish the militants lost during the conflict. Moreover, a logistical organisation needs to be maintained to support the combatant units, by forming dedicated units for this role or by extracting resources from the local population, and often by both. Participating in or providing material support to the rebellion is a risky decision for individuals, with clear risks to lives and income, and unclear returns. Plausible prior grievances or a history of conflict, which is framed and presented as an appealing cause (Galula, 1964), are often what motivates the population to provide recruitment, material, and popular support to the rebel movement. Rebel leadership would need a coherent cause to capitalise on grievances, delivered by the framing of an ideology, disciplining ideas and narratives.

While ideologies can attract and convince people to join or help an organisation, some ideologies go beyond being merely a motivation for the conflict. Ideologies differ in terms of their 'density of blueprints:' Certain ideologies also provide detailed strategies, methods, and institutions to achieve objectives (Gutiérrez-Sanín and Wood, 2014, p. 219).[4] These ideologies propose a change not only in the way of governance, but also in key institutions of the society such as the economic system, educational institutions, religious and personal relations. Their desired end-states deviate substantially from traditional structures, and imposing individuals the desire to bring such a fundamental change requires extensive indoctrination and ideological education (Schubiger and Zelina, 2017). The most prominent examples of such comprehensive ideologies with transformative aims are Marxist-socialist and religious ideologies. For example, militants in an Islamist group are thought about Sharia

[4]Ideology has been studied extensively in civil war literature despite the fact that it is difficult to operationalise and measure. Studies have shown that ideology can play a role in the strategies that rebel groups pursue, the decisions they make, and the targets they attack. See, for example, Drake (1998); Gates (2002); Kalyvas and Balcells (2010); Staniland (2015); Wood and Thomas (2017).

Law, are expected to apply it in their daily lives and make their households abide by it. In Marxist-socialist groups, militants are intensively trained about topics such as the Marxist interpretation of history, and also expected to show full devotion to their cause in their daily lives.

Nationalism and other ideologies lack such comprehensive practices to follow and vary across contexts, in some cases borrowing from religious or leftist ideologies (Wood and Thomas, 2017). Many groups also adopt their ideas and values inspired by different political thoughts and form a 'hybrid' ideology (Drake, 1998, p. 55). Prominent examples include ethnic rebel groups that emphasise religion and true believers in their discourse to appeal to an exclusive religious audience, such as Hamas or Taleban (Polo and Gleditsch, 2016). These groups differ from other ethno-nationalist rebel groups, as they rely on ideological indoctrination and propaganda similarly to the religious groups. They also aim to govern along religious lines and frequently include religious references in their propaganda. The ideologies that rebel groups choose to follow are not independent of the context, from the history of grievances, and from the existing values and ideas in the society. The rebel leadership would choose ideologies that help mobilise and gain support, but the options are limited by likely appeal to people and relevance to their grievances (Gutiérrez-Sanín and Wood, 2014).

Even when grievances clearly predate an insurgency, it is challenging to win people's *minds* and to make them willing to strive not only for rebellion, but also for fundamental social change. Both Marxist-socialist and religious (including ethno-religious) groups usually invest more effort on ideological education and propaganda, to reshape minds as a first step for reshaping society. Given other rival competing ideologies defending the status quo, there is a *war* of ideas. Governments facing rebels with those extreme ideologies tend to engage in counter-efforts directed at affected local populations within counter-insurgency campaigns, which makes connection to locals crucial for governments. Anti-extremist discourse and sometimes promotion of liberal ideas and freedom is often seen as a response by the governments in this domain, aiming to degrade the popular support for the rebellion and undermine

its access to resources. Losing the war of ideas threatens the survival of rebel groups, as it would decrease recruitment and popular support, and rebels are expected to take necessary measures to dominate the ideological propaganda domain, by denying government access and isolating the population, which in turn empowers their echo-chamber. Attacking mass media infrastructure such as radio or TV stations, as well as companies and staff, might be a response among several others by the rebel group in order to limit government outreach. Taking out internet access by targeting fixed or mobile internet networks may also serve the same purpose with the increasing prominence of social media in the last decade.

Nationalist groups are expected to be less vulnerable to anti-rebel propaganda, since they stake claims based on already existing ethnic identities and long-lasting grievances. The strength of ethnic (and linguistic) ties, and not diverting from the traditional way of living and cultural norms puts nationalist groups in an advantageous position in terms of popular support. They do not rely on ideological education and indoctrination of populations to recruit and gain support as much as transformative ideologies do. Overall, I expect that Marxist-socialist, religious, and ethno-religious groups would be more likely to target telecommunication infrastructure compared to groups with nationalist or other ideologies.

It is difficult to identify the motivation behind attacks on telecommunications unless the perpetrator group claims responsibility and communicates its intended purpose for the attack. When the Al-Furqan Brigades attacked a satellite communication centre in Egypt in 2013, they later released a video footage and outlined the reasons for the attack as to *'make the media of disbelief know that we are coming and we are about to end them'* and *'to draw for all of our brothers clear and easy steps in the way of jihad to make it easy for them to follow'* (Barnett, 2013). In 2005, Maoist rebels in Nepal attacked a state television tower transmitting anti-guerilla broadcasts in rebel strongholds (Morning Star, 2005). Al-Shabab and Hizbul-Islam in Somalia attacked and seized two radio stations in 2010 and expressed that they 'must serve Islam' (BBC, 2010).

H2. Marxist-socialist, religious, and ethno-religious groups are more likely to target

telecommunication infrastructure compared to nationalist and other groups.

2.3 Data

I analyse 372 intrastate and internationalised intrastate conflicts in UCDP dyadic dataset, covering the period between 1970-2013.[5] I use information from Terrorism in Armed Conflict (TAC) Project (Fortna, Lotito and Rubin, 2022) to attribute terrorism incidents in GTD to the rebel groups in UCDP data.[6] TAC project provides data on the use of terrorism by rebel groups in civil wars, by identifying terrorist attacks perpetrated by the rebel groups in UCDP dyadic dataset. The unit of analysis is conflict dyad-years, which allows me to consider attributes of the opponent governments and the location of the conflict.

2.3.1 Dependent variable

Data on attacks on telecommunication infrastructure are more likely to suffer from acknowledged problems of conflict event data. Under-reporting of attacks on telecommunications is exacerbated by the relative insignificance of these events, compared to incidents with civilian casualties. While this is often the case for attacks on phone lines or cell phone towers, attacks on radio or TV stations are usually high-profile events. It is also worth noting that telecommunication infrastructure has expanded and technologies have evolved over time, which may lead to an overall positive trend in the number of attacks and changes in the types of targets. I use the events in GTD where target type is coded as 'telecommunications,' which includes attacks on facilities and infrastructure for the transmission of information, like cell phone towers, telephone booths, television transmitters or radio towers (START, 2021). Disaggregating types of targets, I grouped the mass communication facilities –radio and TV stations–

[5]Coups and the USA-Al Qaida dyad are dropped from the analysis considering they do not fit into the framing of civil war (Fortna, Lotito and Rubin, 2018).

[6]TAC data project uses version 1-2014 of UCDP dyadic dataset and the same version is used in this study (Harbom, Melander and Wallensteen, 2008; Themnér and Wallensteen, 2014).

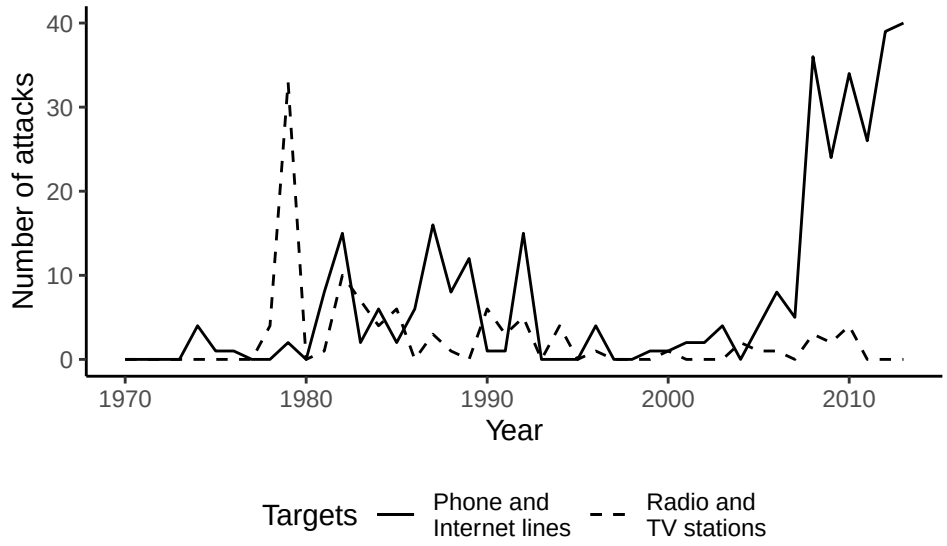


Figure 2.1: Number of attacks to telecommunication infrastructure over time

and phone/internet lines as separate categories, as they might involve different mechanisms discussed above. Figure 2.1 shows the number of attacks over time for each category. The total number of attacks to radio and TV stations is lower than that to phone and internet lines, and attacks to the latter are observed more often in later periods.

Based on the TAC dataset event counts, I created a binary variable that shows if a group had ever targeted telecommunications in a given year. Some events in TAC data are attributed to multiple groups due to the uncertainty of the perpetrator information. I used weights for such events and coded each group as targeted telecommunications if their event count exceeds 1 (see Appendix 2.D.8 for details). I use a binary variable since the aim is to explain the target or tactic choice, rather than the attack frequency (Polo, 2020a). Furthermore, attacks on telecommunications are likely to be underreported. In addition, in many cases rebel groups attack multiple telecommunication targets in different locations simultaneously, which are coded as separate events in GTD. I expect that if a rebel group systematically attacks ICT, at least one event is reported by the news media and captured by coders. Alternatively, I use a proportion variable indicating the share of attacks to telecommunications within all attacks per each group-year, and a count variable showing the number

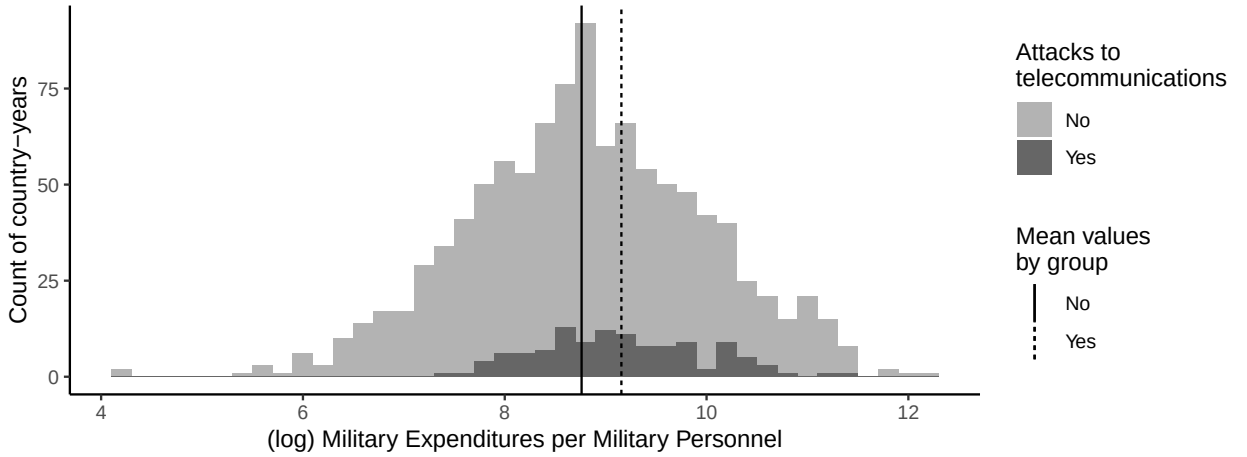


Figure 2.2: Histogram of military expenditures per military personnel (country-year observations)

of attacks to telecommunications. Among the 2017 conflict dyad-years, at least one attack to telecommunications is coded for 146 observations, and 46 out of 372 rebel groups in the dataset targeted telecommunications at least once.

2.3.2 Independent variables

As a measure of the technological sophistication and capabilities of a military, I use *military expenditures per military personnel* from the National Material Capabilities Data of Correlates of War (Singer, 1988). Military expenditures per personnel is a more valid measure than total military spending in terms of the technological advancement of the government forces, as it proxies expenses for arms and equipment which in turn increases capabilities. I lagged this variable for one year to ensure that it is not affected by the attacks on the year of observation, and rescaled it by taking the natural logarithm of the values. Figure 2.2 shows the distribution of the country-year values for this variable, grouped by whether or not any attacks to telecommunications is present, and marking mean values for each group.[7]

I use categories of ideological orientations using information from Polo and Gleditsch (2016), recognising the overlap of different ideologies and providing a rather refined measure.

[7] A Welch t-test confirms the difference between two group means is not equal to zero (p-value $= 2 \times 10^{-8}$).

Figure 2.3: Numbers of rebel groups and ideologies over time

Ethno-nationalist groups advocate secession, autonomy, or concessions for particular groups and have an exclusive ethnic audience. *Ethno-religious* groups differ from ethno-nationalist groups in the emphasis on religion and true believers (Polo and Gleditsch, 2016, p. 820). Other categories include *Marxist-socialist* and *religious* groups, and *other* ideologies as a residual category that covers groups without ideologies, groups that seek regime change without a specific ideology, and right-wing groups.[8] Figure 2.3 shows the number of rebel groups over time grouped by ideologies, and a list of groups coded under each ideology is provided in Appendix 2.C.

2.3.3 Confounders

I include several variables that are likely to be confounders. To account for the higher likelihood of targeting telecommunications in more intense conflicts, I use *Conflict intensity* variable from the UCDP dyadic dataset, which is 'minor' if there are 25-999 battle-related

[8]Although certain right-wing ideologies might also envision transformative changes in the society, this does not apply to the right-wing groups within the scope and time period of the study, which is limited to the rebel groups in an active civil war between 1970-2013.

deaths in a conflict in a given year, and coded as 'war' if it is equal or greater than 1000 (Pettersson, 2020). I also control for the *type of conflict* using the same resource, which is coded as 'intrastate' when one side is a government and the other side is a rebel group, and as 'internationalised intrastate' when there is an involvement of a foreign government with troops in an intrastate conflict.

Telecommunication infrastructure can be located in more isolated and hard-to-reach areas in mountainous regions, leaving them less protected and more vulnerable to attacks by insurgents. To capture the potential effects of geographical features, I used country level data on the proportion of *mountainous terrain* from Fearon and Laitin (2003). Another concern is the variation between countries and within countries over time regarding how large their telecommunication infrastructure is. While it may vary between countries with different levels of development, the infrastructure had possibly grown over time as well. To account for both, the number of *telephone lines (landline and cellular) per 100 people* from Banks and Wilson (2021) included in the analysis as a proxy for the telecommunication infrastructure. Moreover, under-reporting of events might be more likely in countries where the press is not free. I use *media freedom* variable from Polo and Gleditsch (2016), which is a scale from 1 to 3 where higher values indicate less press freedom, compiled from Freedom of the Press data (Freedom House, 2013) and Van Belle (1997). I also control for *population* and *GDP per capita* (lagged for one year) on logarithmic scale using data from Gleditsch (2002).

Enjoying territorial control over an area implies that the rebels are operating freely without being challenged by the government (Kalyvas, 2006), while confrontations with government forces may take place outside the rebel-controlled area. Although spatial variance in rebel control is expected, the probability of attacking infrastructure may be lower on average for groups that enjoy territorial control. To measure *territorial control* at the group level, I created a binary variable using information from Polo and Gleditsch (2016), showing whether or not the group controlled any territory. I include *rebel strength* variable from Cunningham, Gleditsch and Salehyan (2013), which aggregates information regarding the

military strength of rebel groups relative to the government, indicating whether the rebel group is much weaker, weaker, at parity, stronger or much stronger than the government (Cunningham, Gleditsch and Salehyan, 2013, p. 522). An alternative explanation might be the weakness of rebel groups relative to government forces, implying that *terrorism as the weapon of the weak* argument is in effect. Following recoding of Fortna, Lotito and Rubin (2018), the values are approximated to a numerical scale ranging from -2 to 2. Lastly, following Carter and Signorino (2010) I include a cubic spline indicating *time since last attack* to account for temporal dependency. Summary statistics of the variables are presented in Appendix 2.A.

2.4 Analysis

I start by presenting descriptive relationships to explore the empirical associations proposed in the hypotheses. Figure 2.4 plots the dyad-year observations of military expenditures per military personnel in log scale against the number of attacks to telecommunications, displaying a nonparametric locally estimated smoothing (LOESS) curve. It reveals an inverted U-shaped relationship, where the number of attacks increases for about the first three quartiles of the values for military expenditures per personnel, and this relationship turns negative for the fourth quartile. This suggests that a quadratic term may be required to better model the relationship between variables.

Table 2.2 presents the numbers and proportions of conflict dyad-years in which the telecommunication infrastructure is attacked at least once, tabulated across the categories of the ideology variable. While descriptive, these values suggest that Marxist-socialist groups have the highest propensity to attack telecommunication infrastructure, about a six-fold increase compared to ethno-nationalist groups, and a three-fold increase compared to religious groups. Ethno-religous groups have a higher propensity to attack as well, while groups with other ideologies have the lowest. Radio and TV stations are overall targeted in a smaller share

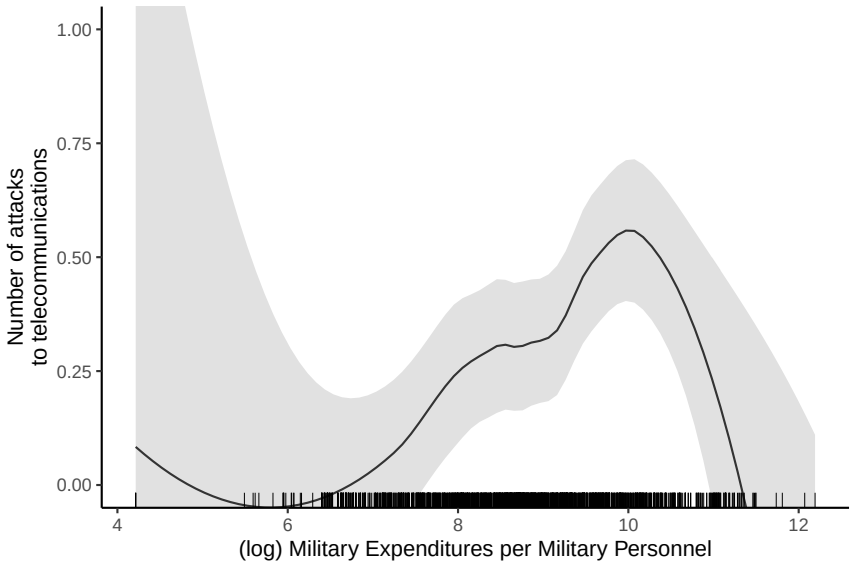


Figure 2.4: Military expenditures per military personnel (log scale) and the number of attacks to telecommunications. Locally estimated smoothing (LOESS) is employed to conflict-dyad year observations.

of incidents, as these facilities are much less in numbers compared to phone and internet lines. In the majority of attacks, phone lines and cell phone towers are targeted, with a higher likelihood by Marxist-socialist and ethno-religous groups compared to others. Marxist-socialist groups also have the highest propensity to attack radio and TV stations. Supporting the expectations, Marxist-socialist, religious, and ethno-religious groups have higher probabilities compared to ethno-nationalist groups and groups with other ideologies. However, religious groups do not exhibit a substantial increase in the probability of attacks.

Attacks to telecommunications	Ethno-nationalist	Ethno-religious	Marxist-socialist	Other ideologies	Religious
No	974	174	292	165	204
Yes	34 (3.4%)	28 (13.9%)	69 (19.1%)	2 (1.2%)	13 (6%)
Radio and TV	12 (1.2%)	5 (2.5%)	19 (5.3%)	1 (0.06%)	5 (2.3%)
Phone and internet	17 (1.7%)	22 (10.9%)	41 (11.4%)	1 (0.06%)	7 (3.2%)

Table 2.2: Number of conflict-dyad years with at least one attack to telecommunications infrastructure

I test both hypotheses across 372 rebel groups and 2017 conflict dyad-years for the pe-

riod between 1970-2013.[9] As observations are nested within countries, standard errors are clustered by country in all analyses. Starting with logistic regression models on targeting telecommunications, Model 1 in Table 2.3 includes a linear term of the military expenditures per personnel and the control variables, while Model 2 has an additional quadratic term. The relationship between targeting telecommunications and military expenditures per personnel is statistically insignificant in Model 1, while the results in Model 2 confirm the inverted U-shaped relationship, yielding statistically significant coefficients for both linear and quadratic terms and also improving the model fit. Model 3 includes all controls and the ideology variable with ethno-nationalist groups as the baseline category. The positive and statistically significant coefficient for the Marxist-socialist category shows an increase in the probability in line with the hypothesis. While the coefficient for the ethno-religious category is also positive, the p-value is slightly above the 0.05 level (0.057). Contrary to propositions, religious groups do not exhibit a significant increase in the probability of targeting telecommunications compared to ethno-nationalist groups. Model 4 is the full model with both independent variables and all covariates. The results are nearly identical with Models 2 and 3, except for a slight decrease in the size of the coefficients for the military expenditures per personnel. The statistical significance of the negative coefficient for other ideologies is driven by the very small number of successes in that category and by clustering standard errors. Overall, the results provide evidence in favour of hypothesis 1 and partially support hypothesis 2. The predicted means for probability of targeting telecommunications are plotted in Figure 2.5, with 0.95 confidence intervals, using Model 4.

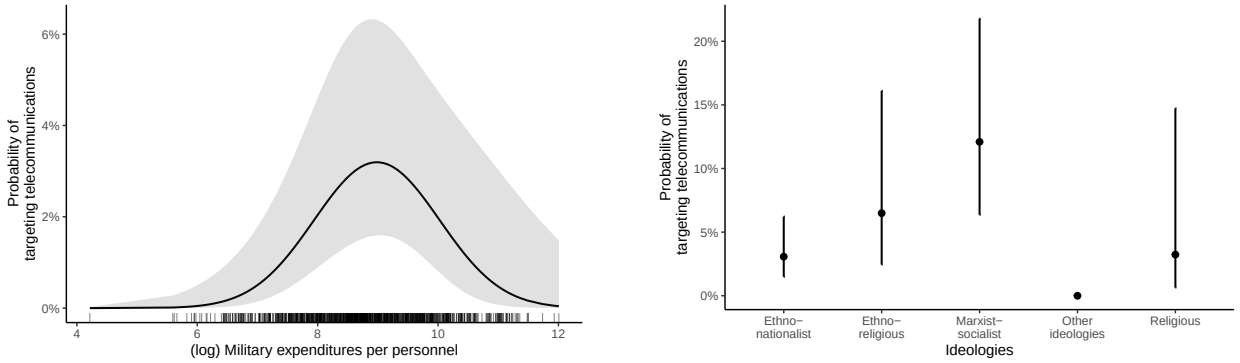
To ensure that the results in the first set of models are not sensitive to the specification of the dependent variable, Model 5 uses the share of attacks to telecommunications within all terrorist attacks of a group as the dependent variable, employing quasi-likelihood to allow for proportions on the left-hand side. Results are similar except for the ethno-religious category, which does not exhibit a meaningful relationship in this specification. The last two

[9]Due to missing values in some variables, analyses are done with fewer observations.

	DV: Binary				DV: Proportion	DV: Count (ZINB)	
	Model 1	Model 2	Model 3	Model 4	Model 5	Count model	Zero model
Intercept	−4.90	−43.42***	−5.09	−41.18***	−57.65***	−74.64***	−36.72
	(3.56)	(11.15)	(3.30)	(11.15)	(16.28)	(17.90)	(35.65)
(log) Military exp. per personnel$_{t-1}$	0.10	9.02***		8.55**	11.79**	15.91***	7.96
	(0.20)	(2.67)		(2.60)	(3.81)	(3.87)	(7.68)
(log) Military exp. per personnel$^2_{t-1}$		−0.51***		−0.48**	−0.64**	−0.91***	−0.51
		(0.15)		(0.15)	(0.21)	(0.20)	(0.43)
Marxist-socialist			1.47***	1.47***	1.42**	3.58***	0.73
			(0.40)	(0.42)	(0.52)	(0.76)	(1.15)
Religious			0.40	0.05	0.35	0.94	−0.24
			(0.75)	(0.80)	(0.69)	(0.91)	(1.43)
Ethnoreligious			0.79†	0.78†	0.66	1.40†	−0.34
			(0.42)	(0.46)	(0.50)	(0.83)	(1.12)
Other ideologies			−1.11	−14.84***	−15.50***		
			(1.16)	(0.57)	(0.51)		
Territorial control	0.29	0.38	0.04	0.07	0.28	−2.36***	−2.62**
	(0.28)	(0.27)	(0.23)	(0.23)	(0.38)	(0.34)	(0.98)
Mountainous terrain (log)	0.62**	0.50**	0.36†	0.27	0.04	−1.49***	−1.65**
	(0.21)	(0.18)	(0.20)	(0.18)	(0.18)	(0.31)	(0.58)
Conflict intensity (war)	1.04***	1.04***	1.07***	1.16***	−0.14	1.32**	−0.88
	(0.29)	(0.26)	(0.29)	(0.25)	(0.25)	(0.48)	(1.00)
Type of conflict (Internationalised)	0.44	0.43	0.55	0.66	−0.16	0.41	−1.87
	(0.68)	(0.65)	(0.69)	(0.64)	(0.54)	(0.96)	(1.39)
Population (log)	0.19	0.13	0.22	0.11	0.05	−0.45***	−0.92*
	(0.18)	(0.16)	(0.14)	(0.13)	(0.16)	(0.12)	(0.45)
GDP per capita$_{t-1}$	0.25	0.24	0.32	0.13	−0.21	1.23***	1.28
	(0.41)	(0.37)	(0.31)	(0.34)	(0.34)	(0.33)	(1.02)
Media freedom	−1.00***	−0.99***	−0.71***	−0.69***	−0.33*	0.39	2.43**
	(0.22)	(0.20)	(0.20)	(0.18)	(0.14)	(0.48)	(0.77)
Tel. lines per 100 people	0.01*	0.02**	0.01*	0.02**	0.01*	0.03***	0.03†
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)
Time since last attack	−0.38**	−0.35**	−0.36**	−0.30**	−0.35**	−0.76*	−0.57
	(0.12)	(0.12)	(0.11)	(0.11)	(0.11)	(0.35)	(0.71)
Time^2	0.02†	0.01	0.02†	0.01	0.02†	0.06	0.07
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.04)	(0.06)
Time^3	−0.17	−0.16	−0.15	−0.09	−0.14	−1.04	−1.42
	(0.16)	(0.16)	(0.14)	(0.14)	(0.14)	(0.82)	(0.89)
AIC	798.66	769.15	801.68	736.40		954.01	954.01
BIC	875.12	851.08	895.89	840.15			
Log Likelihood	−385.33	−369.58	−383.84	−349.20		−440.00	−440.00
Deviance	770.66	739.15	767.68	698.40	17.51		
Num. obs.	1740	1740	1885	1738	1738	1740	1740

***$p < 0.001$; **$p < 0.01$; *$p < 0.05$; †$p < 0.1$.
Errors are clustered at country level for all models

Table 2.3: Regressions on targeting telecommunications



(a) Military expenditures per miltary personnel

(b) Rebel group ideologies

Figure 2.5: Predicted probabilities of targeting telecommunications

columns in Table 2.3 present a zero-inflated negative binomial regression using the counts of attacks on telecommunications as the dependent variable. *Other ideologies* as a residual category is dropped in this model to allow convergence. The findings are similar in the count model, implying that the relationships linked to increasing probabilities in the previous models are relevant for the increasing number of events, while the zero model does not yield any significant estimates for the variables of interest.

Telecommunication infrastructure as a generic term involves different types of technologies that may be related to the specific mechanisms discussed above. In particular, preventing government anti-rebel propaganda may result in attacks to radio or TV stations, especially before the internet era. When attacks to radio and TV stations are used as the dependent variable, results imply that Marxist-socialist and religious groups have a higher probability of targeting mass communication infrastructure, but statistical evidence is limited. Military expenditures per military personnel exhibit a similar relationship across all types of targets, and Marxist-socialist and ethno-religious groups are more likely to attack phone and internet infrastructure as well (see Appendix 2.D.2).

A battery of robustness checks are performed to achieve better confidence on the findings. As a long-running project, GTD had changes in the availability of sources and workflows of data collection over time, in particular in the years 1998, 2008 and 2012 (START, 2021,

p. 4). The results hold when the full model (Model 4) is replicated using subsets split by the years 1998 and 2008, presented in Appendix 2.D.3. The quadratic relationship between military expenditures per personnel and targeting telecommunications is present in all periods, while after 1998 the positive component of this relationship is substantively larger in size. Marxist-socialist groups exhibit higher probability across all subsets. The coefficient for ethno-religious category is positive and significant for the period after 2008, possibly due to an increasing number of groups with this ideology in the later periods. Contrary to expectations, religious groups have significantly lower probability of attacking telecommunications for the period 1998-2008.[10]

TAC data project matches events in GTD to the groups in the UCDP dataset with varying levels of uncertainty. The results hold across all levels, including the least inclusive level which only accounts for direct matches and armed wings of organisations (see Appendix 2.D.8). The relationship between military expenditures per personnel and targeting telecommunications is robust to country and conflict fixed effects. However, as a time-invariant variable, the coefficients for the ideology categories become statistically insignificant once country fixed effects are included. Explanatory variables do not possess enough variance for the results to hold when two-way (country-year) fixed effects are employed. However, results are robust to country-year random effects, rare events logistic regression, and weighted regression by employing 'covariate balancing generalised propensity score' for military expenditures per personnel variable (Fong, Hazlett and Imai, 2018) (see Appendix 2.D.6). Finally, inclusion of the independent variables improves in- and out-of-sample predictive power, and sensitivity tests show that potential unobserved confounders are unlikely to overturn the results (see Appendices 2.D.1 and 2.D.9).

As an alternative explanation, the link between the military capabilities of a government and the insurgent targeting of the telecommunication infrastructure may instead reflect a

[10]Subsets by the phases of GTD data collection effort also overlaps approximately with the changing nature of telecommunication technologies, in particular widespread availability of cell phones and social media use, respectively. This robustness check can also be considered as an investigation of changes in communication technologies over time.

broader shift in the strategy of the insurgents. This implies that rebels may substitute soft targets for military targets if their opponents possess overwhelming superiority, and they avoid battles and commit terrorist attacks more often. To investigate trends of different outcomes of rebel violence, I replicate the main model using battles, battle deaths, and terrorist attacks on various types of target as the dependent variable.[11] Results show that the number of battles and battle deaths are not associated with military expenditures per personnel, while terrorist attacks on civilian targets and other types of infrastructure exhibit a similar inverted U-shaped relationship (see Appendix 2.D.7). Although the target substitution argument cannot be confirmed with the available evidence, it is likely that terrorist tactics, including against military targets, are employed more often against militaries with higher technical capabilities.

2.5 Conclusion

The high pace of technological developments in ICTs motivated extant work in conflict studies, and whether or how it affects conflict is still under investigation. This study aims to contribute to these efforts by focusing on an overlooked aspect of this relationship, the targeting of telecommunication infrastructure by rebel groups. It also contributes to the literature on rebel group target selection by focusing on telecommunications as a particular target type. The results suggest that rebel groups are targeting telecommunications when it constitutes a threat to their survival. A technologically advanced military which can quickly act on the intelligence gained via these networks makes rebel groups more likely to target ICT, over concerns about being detected and targeted by government forces. However, against militaries placed at the high-end of this spectrum, rebels are less likely to target telecommunications and possibly rely on stricter preventive measures, implying a more clandestine approach to insurgency. Furthermore, ambitious ideologies aiming to transform the society and rely too

[11] Information on the number of battles and battle deaths are taken from Uppsala Conflict Data Project Geo-refrenced Event Dataset (GED) (Sundberg and Melander, 2013).

much on propaganda and indoctrination of the masses, in particular Marxist-socialist or ethno-religious ideologies, are strong predictors of targeting telecommunications.

Overall, this study serves as a step towards a better understanding of rebel strategies as a reaction to the dynamics of the conflict. However, there are few limitations. First, the time scope of the study misses much of the social media boom, and we have yet to see the extent of the impact social media have on conflict. It can be an effective tool for rebel groups to convey their message to a wider audience, to spread their propaganda and increase recruitment. Even though a group attacks ICT infrastructure or group leadership tries to limit its militants' use of telecommunication for concerns over security, group leadership itself may continue to have presence in mediums of mass communication, internet or social media. Besides, new technologies such as cloud-based instant messaging applications, provide richer content that is getting closer to face-to-face communication, and may be exploited by rebel groups to their benefit, in terms of within-group communication and organisational effectiveness. Second, under-reporting of events makes a subnational study unfeasible. Such disaggregated studies might be the next step for exploring micro-mechanisms, in particular spatial and temporal variation in attacks of a single rebel group.

Appendix 2.A Summary statistics and the correlation matrix of independent variables

	Missing (%)	Mean	SD	Min	Median	Max
Targeting telecommunications (binary)	3	0.1	0.3	0.0	0.0	1.0
Military expenditures per personnel (log scale)	9	8.7	1.2	4.2	8.8	12.2
Mountainous terrain (log)	0	2.8	1.2	0.0	2.7	4.4
Territorial control (binary)	0	0.4	0.5	0.0	0.0	1.0
Telephone lines per 100 people	0	17.2	33.8	0.0	1.7	199.4
Population (log scale)	0	3.4	1.5	-1.0	3.3	7.2
GDP per capita (log scale)	0	8.0	1.0	6.2	7.9	10.6
Media freedom	1	2.4	0.7	1.0	3.0	3.0
Rebel strength	3	-1.4	0.6	-2.0	-1.0	2.0

categorical variables

		N	%
Intensity level	1 (conflict)	1602	79.4
	2 (war)	415	20.6
Type of conflict	3 (Intrastate)	1693	83.9
	4 (Internationalised intrastate)	324	16.1

Table 2.4: Summary statistics

	Targeting telecom. (binary)	Mil. Exp. per Per.	Mountainous terrain (log)	Territorial control	Tel. lines per 100 people	Population (log)	GDP pc (log)	Media freedom	Rebel strength
Targeting telecom. (binary)	1	.	.	.	.	.	.	.	.
Mil. Exp. per Per.	.10	1	.	.	.	.	.	.	.
Mountainous terrain (log)	.08	-.30	1	.	.	.	.	.	.
Territorial control	.00	-.18	.13	1	.	.	.	.	.
Tel. lines per 100 people	.13	.55	-.17	-.13	1	.	.	.	.
Population (log)	.07	.12	.17	-.13	.06	1	.	.	.
GDP pc (log)	.13	.73	-.29	-.19	.60	-.04	1	.	.
Media freedom	-.16	-.38	.23	.23	-.23	-.20	-.45	1	.
Rebel strength	.01	-.17	-.04	.24	-.13	-.33	-.23	.21	1

Table 2.5: Correlation matrix

Appendix 2.B Additional information on the data

Although data on attacks to telecommunications are likely to suffer from limitations of conflict event data and may not provide complete numbers (Drakos and Gofas, 2006; Weidmann, 2016), it is a useful source for classifying which groups target telecommunications and which do not. There are several reasons why a binary dependent variable is preferred as the main specification. As mentioned in the main text, attacks on telecommunications are likely to be underreported. An example is PKK, which often targets cell phone towers. Although 11 events have been coded in GTD as attacks by PKK on telecommunications, an official statement from the Turkish government in 2015 underlines that there have been 227 attacks on GSM base stations by PKK (Anadolu Ajansi, 2015). Another example is the Taliban, which destroyed 220 telecommunication towers within eight months in 2019, according to a statement by Afghanistan Telecom Regulatory Authority (Nikzad, 2019). However, only two related events are coded in GTD for the period mentioned in the statement. In addition, in many cases rebel groups attack multiple telecommunication targets in different locations simultaneously, which are coded as separate events in GTD. For example, on 5 September 2012, 21 attacks targeted cell phone towers and buildings throughout Nigeria, all of which later were claimed by Boko Haram (Williams and Guttschuss, 2012). More recently, on 22 February 2019, the Communist Party of Nepal-Maoist attacked 28 cell phone towers (START, 2021).

On another note, cyber attacks are neither coded in GTD nor included in the analysis as they are a different type of violence which requires a variety of actor types to be included in the analysis, and they are not conditional on spatial proximity like physical attacks. Such attacks may result from different motivations which are not necessarily political.

The independent variable, military expenditures per miltiary personnel, is also preferable to Composite Index of National Capability (CINC) score in the National Material Capabilities Data of Correlates of War (Singer, 1988), since CINC represents a country's potential

power in total mobilisation rather than actual power, and it captures relative power between states rather than absolute power of a state (Hendrix and Young, 2014, p.342). In the analyses I use a one-year lag of this variable, but one can argue that the purchase of military equipment often takes longer than a year. However, more than half of the military budgets of countries are usually allocated to personnel, operational, and maintenance costs which return as immediate benefits. For example, the level of NATO guidelines for the procurement of military equipment and research and development expenditures is 20% of the defence budgets for each member country, but many countries spend below this threshold (NATO, 2021). Therefore, I consider one-year lag as appropriate.

Finally, coups and the USA-Al Qaida dyad are dropped from the analysis considering they do not fit into the framing of civil war (Fortna, Lotito and Rubin, 2018). Coups are carried out by the military or by a fraction in the military of a government, using the government's own resources and coercive power against itself, and tend to result in a very short time frame. Successful coups may not result in casualties above the threshold of civil wars, and those that generated high casualties are likely to be failed attempts (Cunningham, Gleditsch and Salehyan, 2009). For the USA-Al Qaida conflict, identifying the location and the governments in the dyad is difficult. While the conflict location is coded as the United States in the UCDP data, only the attacks on 9/11 have taken place in the US territory, and other attacks are located in several countries. Troops from more than 20 countries are involved in the fight against Al Qaida. In this untraditional conflict, Al Qaida mainly opposed and targeted the US presence in the Middle East, rather than the governments of the countries where they are active (UCDP, no date).

Appendix 2.C Data on the ideological orientations of the rebel groups

Table 2.6 below presents the shares of ideology categories in Polo and Gleditsch (2016), followed by the list is of groups coded under each ideology.

	Ethno-nationalist	Ethno-religious	Marxist-socialist	Religious
Share of groups	0.47	0.07	0.12	0.09
Share of group-years	0.50	0.10	0.18	0.11
	Regime change no spec. ideo.	No ideology	Right-wing	Coup
Share of groups	0.11	0.04	0.01	0.08
Share of group-years	0.05	0.02	0.01	0.02

Table 2.6: Share of ideology categories

- *Ethno-nationalist (nationalist-separatist)*: UNITA, Palipehutu, CNDD, Frolina, CNDD-FDD , Palipehutu-FNL, MOSANAT, CSNPD, MPS, FNT, MDJT, MPA/Republic of Anjouan, Ninjas, Ntsiloulous, AFDL, RCD, MLC, FRUD, FRUD - AD, TPLF, EPRDF, ALF, ARDUF, EPLF, ONLF, OLF, MPCI, MPIGO, NPFL, INPFL, LURD, MPA, FIAA, POLISARIO, CRA, FDR, FPR, ALiR, MFDC, Kamajors, UPA, HSM, WNBF, FLEC-FAC, FLEC-R, PIRA, JSS/SB, EZLN, Contras/FDN, LTTE, RIRA, Republic of Abkhazia, KDPI, ATTF, NLFT, Republic of Croatia, Croatian irregulars, KDP, Republic of Slovenia, PUK, NSCN-IM, Serbian irregulars, Serbian Republic of Bosnia-Herzegovina, Croatian Republic of Bosnia-Herzegovina, Autonomous Province of Western Bosnia, UCK, ULFA, Republic of South Ossetia, Serbian Republic of Krajina, KIO, KNU, RCSS, MTA, ABSU, NMSP, KNPP, NDFB, God's Army, UWSA, PLA, BMA, PKK, UNLF, BRA, MQM, Fretilin, Chechen Republic of Ichkeria, CPN-M, MODEL, Republic of Nagorno-Karabakh, Military faction (forces of Suret Husseinov), ETA, PMR, Republic of Armenia, APF, Democratic Republic of Yemen, Fatah, LRM,

Sikh insurgents, Hizb-i Wahdat, PFLP, UIFSA, AMB, PNA, PFLP-GC, UNRF II, SLM/A, JEM, EIJM - AS, PJAK, NDPVF, OPM, MIM, TNV, SWAPO, WSLF, Military faction (forces of Samuel Doe), TELO, Republic of Biafra, Mukti Bahini, BLF, APCO, ANC, SLA, ZANU, ZAPU, FNLA, NRA, Royalists, EGP, UFDR, NRF, SLM/A - MM, Baloch Ittehad, BLA, SPLM/A, NDA, CNDP, SLM/A-Unity, ATNMC, BDK, KDP-QM, FAT, ELF, SSLM, EPRLF, Non PLO groups, FUNA, UNRF, UPDA, Lord's Army, PF, LAA, Amal, SSA, SURA, SSNLO, MNJ, SSRA, TRC, FLAA, UFRA, KCP, PREPAK, Military faction (forces of Maldoum Bada Abbas), Rejectionist Front, PLO, NDFB - RD, KNF, KNUP, SLM, RPF, ALP, SALF, LNUP, MNDAA, ANLP, DKBA 5, SSDM/A, IGLF, SPLM/A-North, SSLM/A, Republic of South Sudan, SSPP, FDLR, SRF, MNLA, GNLA, NSCN-K, Kata Katanga, NDFB-S

- *Ethno-religious*: MILF, MNLF, ASG, MNLF - NM, AIAI, RSO, Taleban, GAM, Chechen Republic of Ichkeria, Kashmir insurgents, Wahhabi movement of the Buinaksk district, Forces of Michel Aoun, PIJ, Hamas, Hizb-i Islami-yi Afghanistan, Al-Mahdi Army, ISIS, Patani insurgents, Muslim Brotherhood, RJF, PRC, Jondullah, Hezbollah, MNLF - HM, PULF, Forces of the Caucasus Emirate, ETIM, BIFM

- *Religious*: AIS, Takfir wa'l Hijra, GIA, AQIM, Islamic Legion, LRA, ADF, al-Gama'a al-Islamiyya, SCIRI, al-Qaida , IMU, Jam'iyyat-i Islami-yi Afghanistan, Hizb-i Islami-yi Afghanistan, Junbish-i Milli-yi Islami, Ansar al-Islam, JIG, Ahlul Sunnah Jamaa, Islamic Charter Front, JSM, ARS/UIC, Harakat-i Inqilab-i Islami-yi Afghanistan , Mahaz-i Milli-yi Islami-yi Afghanistan , Jabha-yi Nijat-i Milli-yi Afghanistan , Ittihad-i Islami Bara-yi Azadi-yi Afghanistan , Harakat-i Islami-yi Afghanistan, Hizb-i Islami-yi Afghanistan - Khalis faction, TTP, Al-Shabaab, AQAP, Jama'atu Ahlis Sunna Lidda'awati wal-Jihad, Hizbul Islam, Ansar Dine, TTP - TA, Lashkar-e-Islam, MUJAO, Forces of Mullo Abdullo, Signed-in-blood-Battalion

- *Marxist-socialist*: EPDM, EPRP, CPP, FMLN, URNG, Sendero Luminoso, FARC,

MEK, JVP, AIAI, EPR, CPB, MRTA, Devrimci Sol, ELN, EPL, CPN-M, KR, PWG, MCC, CPI-Maoist, MKP, MLN/Tupamaros, M-19, FPL, ERP, Sudanese Communist Party, Monima , NRC, KNUFNS, PFLO, Yemenite Socialist Party - Abdul Fattah Ismail faction, FSLN, CPM, Montoneros, CPT, NDF, FAR I, EGP, ORPA, CPB-RF, CPI-ML, FAR II, NSF, PDPA, Pathet Lao, Bandera Roja, CPA, PBCP, PBCP-Janajudhha

- *Regime change - no specific ideology*: CNR, MDD, FARF, SNM, SPM, SSDF, USC/SSA, USC/SNA, SRRC, ABSDF, UTO, Lebanese Forces, FRCI, FUCD, RÃ©sistance ArmÃ©e Tunisienne, UNLF, UFM, RAFD, UFDD, NDA, Frolinat, First Liberation Army, Second Liberation Army, FAN, FAP, GUNT, CDR, FLNC, Kikosi Maalum, Fronasa, NUF, AN , CPJP, UFR, PFNR, FDSI-CI, NTC, Forces of Muammar Gaddafi, M23, Seleka, PFT , SPLM/A In Opposition, Syrian insurgents

- *Other - no ideology*: Revolutionary Forces of 1 April , Cocoyes, RFDG, Renamo, RUF, Cobras, MJP, Zviadists, Parliamentary Forces (Russia), OPON Forces, WSB, Military faction (Harar garrison), APCLS, SSDM/A - Cobra Faction, Sultanate of Sulu, Forces of Paul Joseph Mukungubila

- *Right-wing*: KPNLF, FUNCINPEC, FNLA, Lebanese Forces - Hobeika faction, EDU

- *Coup*: Military faction (forces of André Kolingba), Military faction (forces of Amsha Desta and Merid Negusie), Military Junta for the Consolidation of Democracy, Peace and Justice, Military faction (Lesotho), AFRC, Presidential guard (Comoros), Jamaat al-Muslimeen, Military faction (forces of Honasan, Abenina and Zumel), National Guard and Mkhedrioni, Military faction (forces of Himmler Rebu and Guy Francois) , Military faction (forces of Raol Cédras) , Forces of Francois Bozize, NSF, Forces of Khudoberdiyev, FLRN, OP Lavalas (Chimères) , Military faction (forces of Moisés Giroldi) , MTD, Military faction (forces of Andres Rodriguez), Military faction (forces of Hugo Chávez) , Military faction (forces of Shahnawaz Tanay), Popular Front (Burkina Faso),

Military faction (forces of Augusto Pinochet, Toribio Merino and Leigh Guzman) , Military faction (forces of Jerry John Rawlings), Military faction (forces of Ekow Dennis and Edward Adjei-Ampofo) , Military faction (forces of Benjamin Mejia), Military faction (forces of Hezekiah Ochuka), Military faction (forces of Ibrahim Saleh), Military faction (forces of Mohamed Madbouh), Military faction (forces of Idi Amin), Military faction (forces of Charles Arube), Military faction (Red Berets)

Appendix 2.D Robustness checks

2.D.1 Improvements in Predictive Power: ROC and PR Curves

In- and out-of-sample predictive powers of the main models are estimated as the area under the receiver operating characteristic curves (ROC), comparing Model 4 in Table 2.3 with a model including only control variables, in order to assess the additional predictive power gained by introducing explanatory variables, *military expenditures per military personnel* and *ideologies*. Substantial improvements are made, with about 3.3 percentage points increase in in-sample (0.8318 → 0.8657) and out-of-sample (0.814 → 0.847) prediction. Considering positive events in the observed values are proportionally less than non-events, area under the precision-recall (PR) curves is also computed. The scores for the PR curves improved by about 10 percentage points by introducing the two main explanatory variables (In-sample: 0.3087 → 0.4292, out-of-sample: 0.31 → 0.41). Improvements in in-sample prediction are visualised in Figure 2.6.

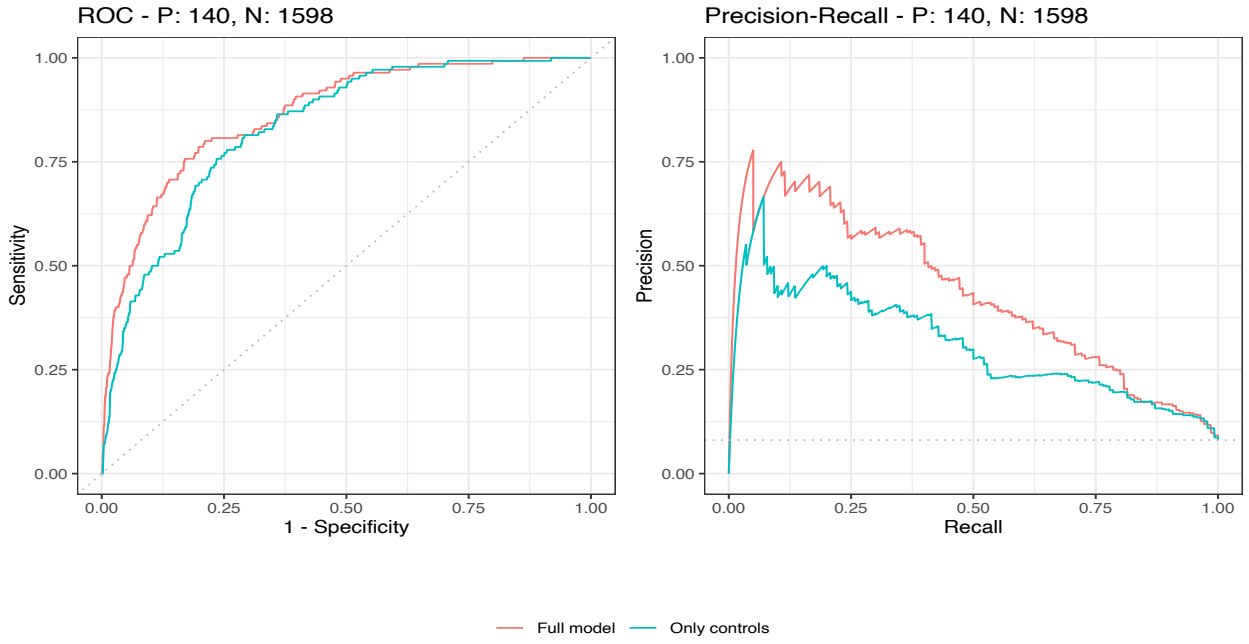


Figure 2.6: ROC and PR curves

2.D.2 Replications with different types of telecommunication infrastructure

	Radio & TV			Phone & Internet		
DV: Binary	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Intercept	-8.34^{*}	-65.42^{**}	-62.76^{**}	-2.06	-39.22^{**}	-37.50^{**}
	(3.52)	(19.95)	(20.59)	(4.00)	(12.64)	(12.69)
(log) Military exp. per personnel$_{t-1}$		13.43^{**}	12.79^{**}		8.43^{**}	8.10^{**}
		(4.74)	(4.75)		(3.21)	(3.07)
(log) Military exp. per personnel$^2_{t-1}$		-0.74^{**}	-0.70^{*}		-0.47^{*}	-0.45^{*}
		(0.27)	(0.27)		(0.19)	(0.18)
Marxist-socialist	$0.87^{\dagger}$		0.71	1.71^{***}		1.83^{***}
	(0.50)		(0.48)	(0.47)		(0.48)
Religious	$0.99^{\dagger}$		0.82	0.23		-0.14
	(0.51)		(0.50)	(0.80)		(0.76)
Ethnoreligious	0.61		0.40	$1.05^{\dagger}$		1.15^{*}
	(0.52)		(0.63)	(0.56)		(0.56)
Other ideologies	-0.09		-14.41^{***}	-15.23^{***}		-14.62^{***}
	(1.17)		(0.60)	(0.66)		(0.69)
Territorial control	-0.18	-0.07	-0.18	0.16	$0.48^{\dagger}$	0.18
	(0.29)	(0.26)	(0.31)	(0.24)	(0.28)	(0.22)
Mountainous terrain (log)	$0.40^{\dagger}$	0.55^{**}	0.42^{*}	0.09	0.26	-0.05
	(0.23)	(0.17)	(0.21)	(0.24)	(0.18)	(0.19)
Conflict intensity (war)	1.30^{***}	1.29^{**}	1.25^{**}	1.02^{**}	1.03^{***}	1.14^{***}
	(0.37)	(0.39)	(0.40)	(0.31)	(0.25)	(0.25)
Type of conflict (Internationalised)	-0.38	-0.87	-0.99	0.89	0.86	1.21
	(0.85)	(1.31)	(1.24)	(0.93)	(0.84)	(0.78)
Population (log)	-0.11	-0.23	$-0.25^{\dagger}$	0.22	0.15	0.13
	(0.16)	(0.18)	(0.15)	(0.16)	(0.20)	(0.15)
GDP per capita$_{t-1}$	0.67^{*}	0.34	0.34	-0.09	-0.00	-0.16
	(0.34)	(0.40)	(0.38)	(0.41)	(0.47)	(0.42)
Media freedom	-0.63^{*}	-0.85^{***}	-0.75^{**}	-0.77^{**}	-1.04^{***}	-0.68^{**}
	(0.27)	(0.24)	(0.27)	(0.24)	(0.23)	(0.21)
Tel. lines per 100 people	-0.00	0.01	0.01	0.02^{**}	0.02^{**}	0.02^{***}
	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)
Time since last attack	$-0.34^{\dagger}$	-0.23	-0.20	-0.41^{**}	-0.42^{**}	-0.36^{*}
	(0.20)	(0.21)	(0.21)	(0.15)	(0.16)	(0.14)
Time^2	0.02	0.01	0.01	$0.02^{\dagger}$	$0.02^{\dagger}$	0.02
	(0.02)	(0.02)	(0.02)	(0.01)	(0.01)	(0.01)
Time^3	-0.22	-0.11	-0.05	-0.18	-0.23	-0.14
	(0.42)	(0.40)	(0.37)	(0.17)	(0.18)	(0.17)
AIC	362.97	325.01	327.41	552.04	550.83	521.12
BIC	457.18	406.93	431.16	646.25	632.75	624.87
Log Likelihood	-164.48	-147.50	-144.71	-259.02	-260.41	-241.56
Deviance	328.97	295.01	289.41	518.04	520.83	483.12
Num. obs.	1885	1740	1738	1885	1740	1738

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\dagger}p < 0.1$.
Errors are clustered at country level.

Table 2.7: Logistic regressions on attacks to different types of telecommunication infrastructure

2.D.3 Replications with different subsets of time periods

	DV: Binary		
	1970-1998	1998-2008	2008-2013
Intercept	-39.76 (13.00)**	-80.63 (32.08)*	-88.21 (44.23)*
(log) Military exp. per personnel$_{t-1}$	7.83 (3.49)*	18.17 (7.46)*	19.04 (9.47)*
(log) Military exp. per personnel$^2_{t-1}$	-0.43 (0.20)*	-1.10 (0.43)*	-0.94 (0.50)†
Marxist-socialist	1.64 (0.58)**	1.23 (0.45)**	2.99 (0.87)***
Religious	-1.02 (1.30)	-16.06 (1.57)***	0.20 (1.45)
Ethnoreligious	-0.40 (0.85)	0.76 (0.71)	2.74 (1.06)**
Other ideologies	-14.00 (0.57)***	-12.99 (1.16)***	-17.48 (1.66)***
Territorial control	0.11 (0.30)	1.35 (0.58)*	-0.43 (0.95)
Mountainous terrain (log)	0.31 (0.24)	1.06 (0.50)*	-0.13 (0.27)
Conflict intensity (war)	1.37 (0.43)**	1.44 (0.62)*	0.95 (1.36)
Type of conflict (Internationalised)		1.52 (0.93)	2.11 (0.72)**
Population (log)	-0.05 (0.19)	0.59 (0.19)**	0.12 (0.15)
GDP per capita$_{t-1}$	0.24 (0.63)	0.14 (0.56)	-1.23 (0.69)†
Media freedom	-0.83 (0.24)***	-1.41 (0.40)***	0.89 (0.64)
Tel. lines per 100 people	0.03 (0.04)	0.03 (0.02)†	0.01 (0.01)
Time since last attack	-0.16 (0.17)	0.00 (0.16)	-0.45 (0.28)
Time^2	0.00 (0.02)	-0.01 (0.02)	0.02 (0.02)
Time^3	0.07 (0.47)	0.44 (0.36)	-0.13 (0.29)
AIC	409.09	191.90	148.42
BIC	500.43	269.67	210.89
Log Likelihood	-186.54	-76.95	-55.21
Deviance	373.09	153.90	110.42
Num. obs.	1182	443	198

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\dagger}p < 0.1$.
Errors are clustered at country level.

Table 2.8: Regressions on targeting telecommunications with subsets of different time periods

2.D.4 Interacting ideologies with government censorship and media bias indicators from V-dem

Government anti-rebel propaganda may sometimes be accompanied by efforts to deny rebel propaganda by employing censorship or restricting the media. Thus, government censorship efforts or media bias in a country may indirectly indicate the presence of anti-rebel propaganda. Using 'government censorship effort (*v2mecenefm*)' and 'media bias (*v2mebias*)' indicators from the V-Dem project (Coppedge et al., 2022), I replicate the main model including an interaction of the ideology variable with each indicator. The results presented

in Table 2.9 indicate that the government's censorship efforts and media bias in a country can increase the probability of targeting the telecommunication infrastructure by religious groups, while this effect does not resonate among Marxist-socailist groups. Although with limited evidence, the results suggest that ethno-religious groups may be less likely to attack when government censorship efforts are prominent.

	DV: Binary	
	Gov't Censorship	Media Bias
Intercept	-39.835 (11.882)***	-36.186 (11.472)**
(log) Military exp. per personnel$_{t-1}$	8.222 (2.847)**	7.440 (2.840)**
(log) Military exp. per personnel$^2_{t-1}$	-0.452 (0.165)**	-0.414 (0.164)*
Marxist-socialist	1.396 (0.473)**	1.663 (0.591)**
Religious	-0.377 (0.526)	-0.601 (0.827)
Ethnoreligious	1.105 (0.462)*	1.261 (0.566)*
Other ideologies	-15.202 (0.590)***	-14.921 (0.540)***
Marxist-socialist × Gov't censorship effort	-0.172 (0.304)	
Religious × Gov't censorship effort	1.321 (0.671)*	
Ethnoreligious × Gov't censorship effort	-0.461 (0.268)†	
Other ideologies × Gov't censorship effort	-0.443 (0.432)	
Marxist-socialist × Media bias		-0.264 (0.389)
Religious × Media bias		1.154 (0.638)†
Ethnoreligious × Media bias		-0.401 (0.284)
Other ideologies × Media bias		-0.684 (0.311)*
Territorial control	0.201 (0.326)	0.210 (0.267)
Mountainous terrain (log)	0.334 (0.180)†	0.359 (0.184)†
Conflict intensity (war)	1.258 (0.263)***	1.253 (0.248)***
Type of conflict (Internationalised)	0.810 (0.616)	0.536 (0.596)
Population (log)	-0.030 (0.120)	-0.068 (0.124)
GDP per capita$_{t-1}$	0.035 (0.306)	-0.000 (0.340)
Media freedom	-0.511 (0.204)*	-0.381 (0.172)*
Tel. lines per 100 people	0.013 (0.006)*	0.014 (0.006)*
Time since last attack	-0.254 (0.095)**	-0.247 (0.108)*
Time^2	0.009 (0.007)	0.008 (0.008)
Time^3	-0.052 (0.122)	-0.037 (0.141)
AIC	721.392	715.851
BIC	852.443	846.903
Log Likelihood	-336.696	-333.925
Deviance	673.392	667.851
Num. obs.	1738	1738

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\dagger}p < 0.1$.
Errors are clustered at country level.
Both 'government censorship effort' (v2mecenefm) and 'media bias' (v2mebias) indicators are taken from V-Dem project.

Table 2.9: Interacting ideologies with censorship and media bias indicators

2.D.5 Fixed effects models

	DV: Binary		
	Country FE	Conflict FE	Country-Year FE
(log) Military exp. per personnel$_{t-1}$	0.164 (0.089)†	0.148 (0.081)†	0.145 (0.089)
(log) Military exp. per personnel$^2_{t-1}$	−0.009 (0.005)†	−0.009 (0.005)†	−0.008 (0.005)
Marxist-socialist	0.041 (0.039)		0.043 (0.043)
Religious	−0.101 (0.079)		−0.099 (0.072)
Ethnoreligious	0.019 (0.039)		0.029 (0.044)
Other ideologies	−0.040 (0.032)		−0.016 (0.029)
Territorial control	0.004 (0.026)		−0.012 (0.024)
Conflict intensity (war)	0.050 (0.025)*	0.047 (0.033)	0.054 (0.025)*
Type of conflict (Internationalised)	0.046 (0.024)†		0.028 (0.025)
Population (log)	0.196 (0.057)***	0.332 (0.126)**	−0.125 (0.135)
GDP per capita$_{t-1}$	0.023 (0.038)	0.020 (0.036)	−0.034 (0.045)
Media freedom	−0.049 (0.027)†	−0.055 (0.037)	−0.048 (0.029)
Tel. lines per 100 people	0.001 (0.001)	0.000 (0.001)	−0.000 (0.001)
Time since last attack	−0.015 (0.007)*	−0.007 (0.007)	
Time^2	0.001 (0.000)	−0.000 (0.000)	
Time^3	−0.006 (0.007)	0.003 (0.007)	
Num. obs.	1739	1789	1739
R^2 (full model)	0.277	0.401	0.288
R^2 (proj model)	0.083	0.030	0.036
Adj. R^2 (full model)	0.237	0.249	0.229
Adj. R^2 (proj model)	0.073	0.023	0.028
Num. groups: location	76		76
Num. groups: dyadid		352	
Num. groups: year			43

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\dagger}p < 0.1$.
Errors are clustered at conflict level.

Table 2.10: Fixed effects models

2.D.6 Other robustness checks

	DV: Binary		
	Country-Year Random Effects	Rare Events Logit	CBGPS ‡
Intercept	-0.998 (0.319)**	-41.668 (9.126)***	-28.649 (11.746)*
(log) Military exp. per personnel$_{t-1}$	0.217 (0.072)**	8.433 (2.044)***	5.341 (2.592)*
(log) Military exp. per personnel$^2_{t-1}$	-0.012 (0.004)**	-0.469 (0.114)***	-0.272 (0.149)†
Marxist-socialist	0.084 (0.022)***	1.884 (0.287)***	2.323 (0.648)***
Religious	-0.065 (0.032)*	0.367 (0.451)	1.212 (1.072)
Ethnoreligious	0.051 (0.026)†	1.042 (0.341)**	1.496 (0.675)*
Other ideologies			-13.826 (0.564)***
Territorial control	-0.011 (0.017)	0.014 (0.240)	0.402 (0.302)
Mountainous terrain (log)	0.011 (0.013)	0.197 (0.126)	0.202 (0.204)
Conflict intensity (war)	0.051 (0.017)**	1.223 (0.265)***	1.659 (0.258)***
Type of conflict (Internationalised)	0.026 (0.025)	0.744 (0.410)†	0.184 (0.538)
Population (log)	0.039 (0.013)**	0.148 (0.082)†	-0.040 (0.118)
GDP per capita$_{t-1}$	0.016 (0.017)	0.202 (0.186)	0.220 (0.314)
Media freedom	-0.045 (0.015)**	-0.650 (0.172)***	-0.824 (0.193)***
Tel. lines per 100 people	0.001 (0.000)***	0.016 (0.004)***	0.013 (0.008)
Time since last attack		-0.280 (0.092)**	-0.904 (0.178)***
Time^2		0.010 (0.007)	0.060 (0.011)***
Time^3		-0.067 (0.138)	-0.924 (0.162)***
AIC	204.464	723.947	
BIC	302.774	822.257	
Log Likelihood	-84.232	-343.974	
Num. obs.	1740	1740	1738
Num. groups: location	75		
Num. groups: year	43		
Var: location (Intercept)	0.015		
Var: year (Intercept)	0.000		
Var: Residual	0.057		
Deviance		687.947	0.327

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\dagger}p < 0.1$.
Standard errors are clustered at country level for Model 3.
‡ `CBPS` package in `R` used for this analysis (Fong et al., 2021).

Table 2.11: Robustness checks

2.D.7 Replications with different outcomes and alternative explanations

Table 2.12 below presents replications with different outcomes and alternative explanations. I replicate the main model (Model 4 in Table 2.3) using battles, battle deaths,[12] all terrorist attacks, terrorist attacks on civilian targets,[13] terrorist attacks on the other types of infrastructure[14] as the dependent variable. Results show that the number of battles and battle deaths is not associated with military expenditures per personnel, while terrorist attacks on civilian targets and other types of infrastructure exhibit a similar inverted U-shaped relationship. Although the target substitution argument can not be confirmed with the available evidence, it is likely that terrorist tactics, including against military targets, are employed more often against militaries with higher technical capabilities.

Potential alignment between the local population and the government may offer an alternative to the argument that groups with transformative ideologies are more vulnerable to anti-rebel propaganda and more likely to attack telecommunications. If the constituency claimed by the rebels have developed ties with the government, this can as well leave the rebels vulnerable to anti-rebel propaganda. To test this, I coded *exclusion* as a binary variable indicating whether associated ethnic constituencies of rebel groups are excluded from access to state power for each conflict-year observation, using the ACD2EPR dataset (Vogt et al., 2015).[15] I then replicated the main model (Model 4 in Table 2.3) replacing the ideology variable with exclusion. The result is presented in the rightmost column of the Table 2.12. Although the direction of the coefficient of exclusion is negative, it is statistically insignificant,

[12]Information on the number of battles and battle deaths are taken from Uppsala Conflict Data Project Geo-refrenced Event Dataset (GED) (Sundberg and Melander, 2013).

[13]'Civilian targets' include all GTD events except attacks to government (target type = 2), police (target type = 3), military targets (target type = 4), terrorist/non-state militias (target type = 17), viloent political parties (target type = 22) and telecommunications (target type = 16).

[14]Target types in GTD that are included in 'other infrastructure': food and water supplies (target type = 9), utilities (target type = 21), bridge/car tunnels (subtarget type = 103), highway/road/toll/traffic signals (subtarget type = 104).

[15]Following the EPR core dataset's definition, I code the group as excluded if its status is coded as 'powerless', 'discrimination' or 'self-exclusion'.

providing weak evidence in favour of this alternative explanation.

	DV: (log) Count				DV: Binary	
	Battles (GED)	Battle deaths (GED)	All attacks (GTD)	Attacks to civilian targets	Attacks to other infrastructure	Ethnic Exclusion as IV
Intercept	1.96	−2.46	−10.04**	−8.83**	−31.74***	−35.13**
	(2.62)	(5.12)	(3.44)	(3.13)	(7.88)	(12.22)
(log) Military exp. per personnel$_{t-1}$	−0.45	1.18	1.81*	1.66*	5.29**	6.75*
	(0.55)	(1.01)	(0.81)	(0.72)	(1.70)	(2.87)
(log) Military exp. per personnel$^2_{t-1}$	0.02	−0.07	−0.10*	−0.09*	−0.29**	−0.38*
	(0.03)	(0.06)	(0.05)	(0.04)	(0.10)	(0.17)
Ethnic exclusion						−0.52
						(0.38)
Marxist-socialist	0.54***	1.05***	0.70**	0.58*	1.04*	
	(0.15)	(0.26)	(0.26)	(0.25)	(0.41)	
Religious	0.67***	1.47***	0.38	0.32	−0.01	
	(0.20)	(0.41)	(0.52)	(0.46)	(0.77)	
Ethnoreligious	0.67*	0.87*	0.52	0.42	−0.05	
	(0.33)	(0.37)	(0.37)	(0.31)	(0.36)	
Other ideologies	−0.35	−0.00	0.10	0.05	0.87	
	(0.25)	(0.45)	(0.29)	(0.27)	(0.77)	
Territorial control	0.20	0.33	−0.27	−0.25	0.05	−0.28
	(0.17)	(0.24)	(0.18)	(0.17)	(0.36)	(0.51)
Mountainous terrain (log)	0.12†	0.05	0.10	0.11	0.24†	0.55*
	(0.07)	(0.13)	(0.08)	(0.07)	(0.14)	(0.26)
Conflict intensity (war)	1.69***	2.63***	0.67**	0.64***	1.21***	1.05**
	(0.19)	(0.31)	(0.21)	(0.19)	(0.21)	(0.33)
Type of conflict (Internationalised)	0.47*	0.75*	−0.21	−0.15	0.24	0.74
	(0.23)	(0.38)	(0.24)	(0.21)	(0.40)	(0.53)
Population (log)	0.13***	0.02	0.20**	0.14*	0.19†	0.23*
	(0.04)	(0.08)	(0.08)	(0.07)	(0.11)	(0.11)
GDP per capita$_{t-1}$	0.27*	0.12	0.55**	0.45**	0.70**	0.49*
	(0.12)	(0.27)	(0.18)	(0.16)	(0.26)	(0.23)
Media freedom	0.06	−0.33*	−0.50***	−0.44***	−0.27	−0.96***
	(0.13)	(0.16)	(0.15)	(0.13)	(0.20)	(0.28)
Tel. lines per 100 people	0.01**	0.01*	0.01	0.01†	0.01†	0.02*
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.01)
Time since last attack	0.08**	0.14**	−0.11**	−0.10*	−0.10	−0.35*
	(0.03)	(0.05)	(0.04)	(0.04)	(0.07)	(0.17)
Time^2	−0.01***	−0.01**	0.01*	0.01*	0.01	0.01
	(0.00)	(0.00)	(0.00)	(0.00)	(0.01)	(0.01)
Time^3	0.12***	0.20**	−0.11†	−0.11†	−0.07	−0.12
	(0.03)	(0.06)	(0.06)	(0.06)	(0.10)	(0.23)
R^2	0.46	0.39	0.45	0.41		
Adj. R^2	0.45	0.38	0.45	0.41		
Num. obs.	987	987	1738	1738	1738	1423
AIC					1516.11	516.13
BIC					1619.86	600.30
Log Likelihood					−739.06	−242.07
Deviance					1478.11	484.13

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$; $^{\dagger}p < 0.1$.
Errors are clustered at country level.
Target types included in 'other infrastructure': food and water supplies (target type = 9), utilities (target type = 21), bridge/car tunnels (subtarget type = 103), highway/road/toll/traffic signals (subtarget type = 104).
'Civilian targets' include all GTD events except attacks to government (target type = 2), police (target type = 3), military targets (target type = 4), terrorist/non-state militias (target type = 17), viloent political parties (target type = 22) and telecommunications (target type = 16).
UCDP Georefrenced Event Dataset is used for information on battles and battle deaths (Models 1 and 2), which covers the period after 1989. Thus time scope of these models is 1989-2013.

Table 2.12: Replications with different outcomes and alternative explanations

2.D.8 Alternative measurements of the dependent variable in terms of coding uncertainty

Terrorism in Armed Conflict (TAC) project matches each event occurred in conflict countries to UCDP actors using the perpetrator information, and in case perpetrator information is limited (e.g. coded as a generic name such as 'Maoists' or 'unknown') it attributes those events to the possible UCDP actors with a specified method and different uncertainty level (Fortna, Lotito and Rubin, 2022). Matching events with perpetrator groups is done using case specific knowledge, relying on UCDP Conflict Encyclopedia, descriptions of the Non-State Actor database (Cunningham, Gleditsch and Salehyan, 2009), the Terrorist Organisation Profiles (Asal et al., 2019) and other sources. If an event cannot be attributed to a certain rebel group, it is matched with the active groups in the location of attack. An implication of this coding decision is that some events are attributed to multiple groups in multiparty conflicts. However, the authors point out the drawback of duplication and recommend dividing these events by the number of groups that are matched (Fortna, Lotito and Rubin, 2022, p. 6). Following their suggestion, I weighted those events by dividing the number of groups to which they are attributed (e.g., if the same event is attributed to three separate groups, I counted this as 0.33 events for each group.). Considerable amount of information would be lost by dropping these observations. Several groups have over two dozen duplicated events assigned to them, and considering these as they have not attacked telecommunications is less plausible. However, this decision does not affect the results of the analysis, and the results are similar when these events are discarded altogether.

Table 2.13 below shows replication of the main model (Model 4 in Table 2.3) using different levels of coding uncertainty levels in TAC project. Model names represent coding levels of event-group matches: Inclusion criteria is the least restrictive in level F (which is used in the analyses in the main text) and most restrictive in level A. Level D includes connected groups although there is uncertainty or change in the relationship over time. Match level C includes

allies and affiliates. Level B includes factions or umbrella organisations. Level A consist of direct matches and armed wings and is the most restrictive match level in TAC project.

	DV: Binary			
	D	C	B	A
Intercept	−41.04 (11.78)***	−40.65 (11.60)***	−40.65 (11.60)***	−39.95 (11.68)***
(log) Military exp. per personnel$_{t-1}$	8.18 (2.68)**	8.05 (2.63)**	8.05 (2.63)**	7.96 (2.62)**
(log) Military exp. per personnel$^2_{t-1}$	−0.43 (0.15)**	−0.42 (0.15)**	−0.42 (0.15)**	−0.41 (0.15)**
Marxist-socialist	1.91 (0.45)***	1.99 (0.44)***	1.99 (0.44)***	1.92 (0.47)***
Religious	0.18 (0.99)	0.24 (0.98)	0.24 (0.98)	0.21 (0.95)
Ethnoreligious	0.57 (0.49)	0.62 (0.50)	0.62 (0.50)	0.60 (0.51)
Other ideologies	−14.35 (0.58)***	−14.29 (0.59)***	−14.29 (0.59)***	−14.38 (0.58)***
Territorial control	−0.21 (0.27)	−0.19 (0.27)	−0.19 (0.27)	−0.23 (0.28)
Mountainous terrain (log)	0.22 (0.18)	0.19 (0.18)	0.19 (0.18)	0.17 (0.18)
Conflict intensity (war)	1.53 (0.31)***	1.57 (0.30)***	1.57 (0.30)***	1.62 (0.30)***
Type of conflict (Internationalised)	0.82 (0.71)	0.87 (0.72)	0.87 (0.72)	0.83 (0.71)
Population (log)	0.08 (0.14)	0.10 (0.14)	0.10 (0.14)	0.10 (0.14)
GDP per capita$_{t-1}$	0.11 (0.39)	0.13 (0.40)	0.13 (0.40)	0.05 (0.40)
Media freedom	−0.90 (0.23)***	−0.91 (0.23)***	−0.91 (0.23)***	−0.87 (0.25)***
Tel. lines per 100 people	0.01 (0.01)	0.01 (0.01)	0.01 (0.01)	0.01 (0.01)
Time since last attack	−0.27 (0.09)**	−0.28 (0.08)***	−0.28 (0.08)***	−0.32 (0.08)***
Time^2	0.01 (0.01)	0.01 (0.01)†	0.01 (0.01)†	0.01 (0.01)*
Time^3	−0.07 (0.12)	−0.09 (0.12)	−0.09 (0.12)	−0.11 (0.12)
AIC	591.33	582.45	582.45	563.04
BIC	695.08	686.20	686.20	666.79
Log Likelihood	−276.67	−272.22	−272.22	−262.52
Deviance	553.33	544.45	544.45	525.04
Num. obs.	1738	1738	1738	1738

***$p < 0.001$; **$p < 0.01$; *$p < 0.05$; †$p < 0.1$.
Errors are clustered at country level.
Inclusion criteria is the least restrictive in level F and most restrictive in level A. Level D includes connected groups although there is uncertainty or change in the relationship over time. Match level C includes allies and affiliates. Level B includes factions or umbrella organisations. Level A consist of direct matches and armed wings and is the most restrictive match level in TAC project.

Table 2.13: Regressions with alternative measurements of the DV (Different uncertainty levels in TAC project)

2.D.9 Sensitivity tests

Following Cinelli and Hazlett (2020), hypothetical scenarios of unobserved confounding are estimated taking *conflict intensity* and *media freedom* variables as references, to check the fragility of the results. This method is designed for OLS models, therefore Model 4 in Table 2.3 is estimated as a linear probability model to perform the sensitivity analysis. Compared to reference confounders, an unobserved confounder that is 20 times strongly associated with the outcome and military expenditures per personnel would still be insufficient to eliminate

the statistical significance of the coefficient of the latter (Figure 2.7). Similarly, the coefficient estimate for the Marxist-socialist category in the ideology variable would remain statistically significant even when an unobserved confounder is introduced to estimation that is five times strongly associated with the outcome and Marxist-socialist ideologies as each of the two reference variables (Figure 2.8). Sensitivity tests are conducted using `sensemakr` package in `R` (Cinelli, Ferwerda and Hazlett, 2020).

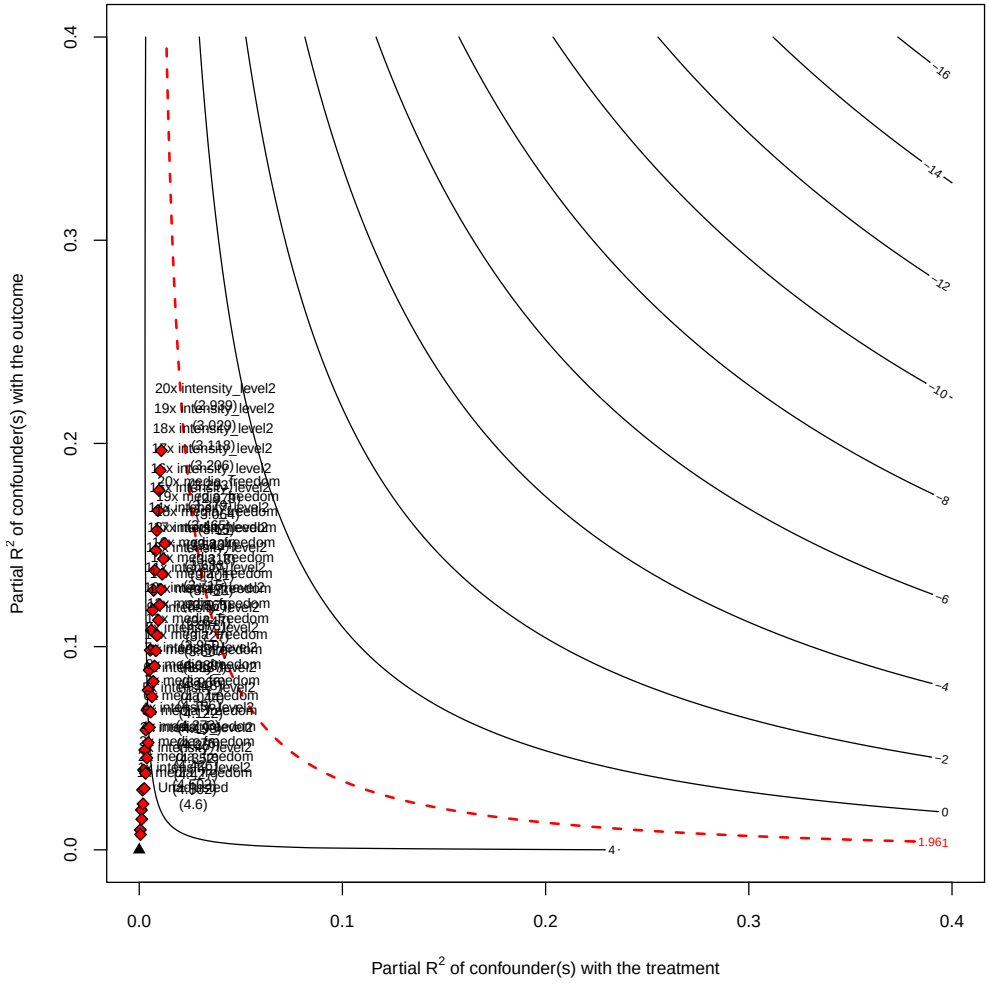


Figure 2.7: Sensitivity test for *military expenditures per military personnel*

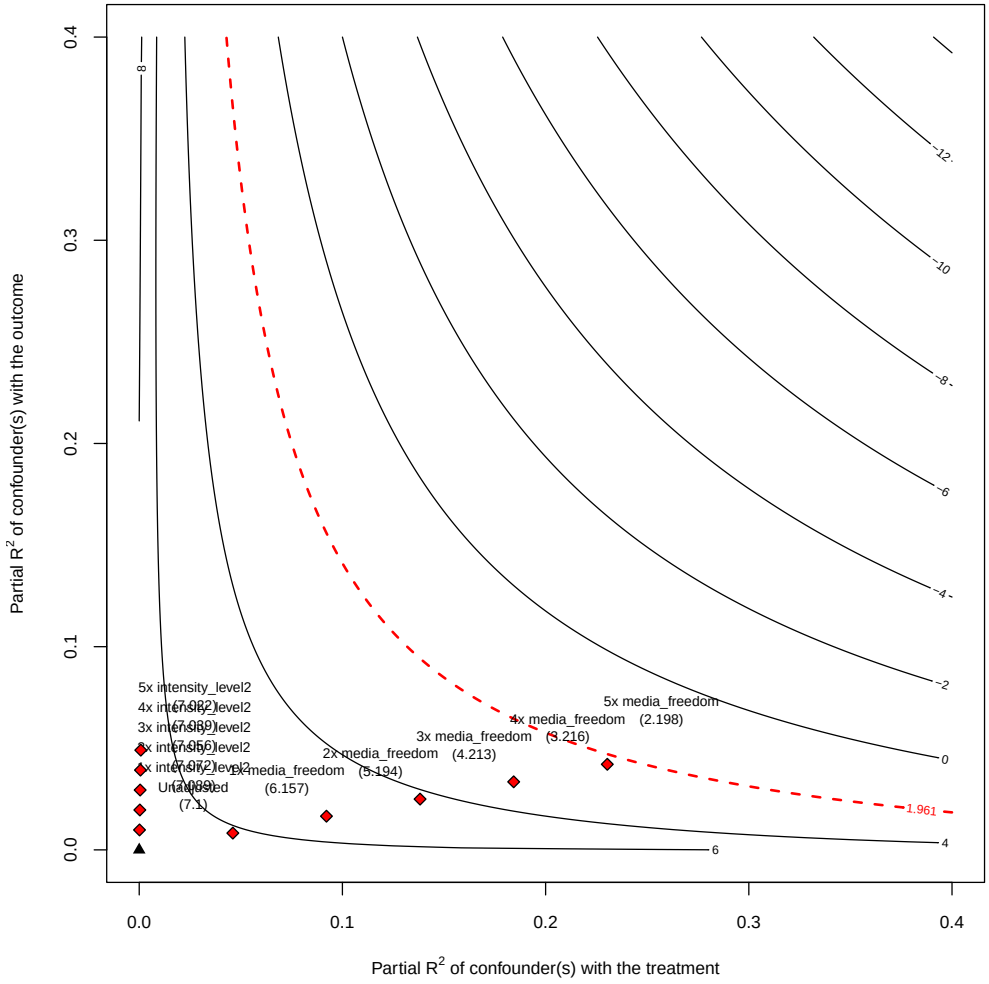


Figure 2.8: Sensitivity test for *Marxist-socialist ideology*

Chapter 3

Did 3G Make Afghan Insurgents Fight More Effectively? A Disaggregated Study

Abstract

Studies on the impacts of communication technologies on civil conflict often focus on the presence of cell phone networks and draw mixed conclusions, suggesting that any potential impact may depend on other important attributes in each context. The prominent theoretical expectation is that cell phones improve collective action. Meanwhile, communication technologies have been advancing and the nature of telecommunication has changed. I argue that the richness of information exchange marked by the introduction of 3G mobile technologies provides an opportunity to push the debate forward, by leading to an increase in the violence of insurgent groups in a high-intensity episode of a civil war. I focus on Afghanistan as a tough test for my argument. Analysing the effect of introducing the 3G network into existing 2G network areas using matched wake analysis and spatial models, I find that the introduction of 3G is associated with an increase in the number of violent events, IED attacks, and coordinated multiple attacks perpetrated by Afghan insurgents. The results are robust to different sizes of spatial units, placebo tests, and less likely to suffer from reporting bias.

3.1 Introduction

The introduction of third-generation (3G) mobile technologies was a significant step toward a new generation of communication technology, marking the transition from mobile phones to 'smartphones.'[1] The higher rate of information transfer capacity made video calls and messages and mobile internet access possible, and facilitated the exchange of information with richer content. With subsequent generations such as 4G and 5G, the bandwidth of communication and richness of content increased exponentially, becoming the closest medium to face-to-face communication.

The use of communication technologies in the context of an intrastate conflict is often linked to improved collective action, which implies an increase in violence. In conflict studies, the impact of communication technologies has so far been studied within the framework of the presence versus the absence of these technologies. The prominent case in these studies is cell phone networks, of which the last two decades have witnessed rapid expansion. Presence of such technologies has been argued to make the formation and sustainment of a rebel group more feasible than before by making cooperation and coordination within groups easier (Bailard, 2015; Pierskalla and Hollenbach, 2013; Walter, 2017). It is also argued that governments can take advantage of these technologies to suppress rebellion (Gohdes, 2020; Shapiro and Weidmann, 2015), and findings showing an increase in rebel violence may be driven by reporting bias (Weidmann, 2016).

I argue that the new generation of communication technologies has generated a substantial variation in the impact they could have on conflict. This is expected to be more significant in the case of moving to the 3G network, which changed the nature of mobile communications

[1]Generations of mobile network technology represent sets of technological implementation standards. Subsequent generations have allowed for more users per cell, higher data transmission rates, and more robust encryption algorithms. The only limitation of new generations is the radius of coverage. Global System for Mobile Communication (GSM) is the most common type of second generation (2G) mobile network. Universal Mobile Telecommunications System (UMTS) is the core of the 3G standard. While CDMA and EDGE technologies are in between the two, they are considered advanced branches of the 2G network.

and represents a bold step forward to a medium close to face-to-face communication. The case of 3G also offers an opportunity to further push the debate. First, while it provides new capabilities to rebels as a commercial technology, for governments, it does not bring novel advantages over the older 2G network. Government forces already use non-commercial technologies for within group communication, and for the population who denounce rebels, 3G did not bring any meaningful difference. Furthermore, the 3G network is almost always introduced in areas already having 2G, and comparing two networks may help mitigate potential biases and endogeneity concerns over comparing areas with and without network connection. In particular, reporting bias is expected to be less severe since both areas of comparison are connected to a network, while the close proximity of both networks may attenuate selection bias.

From the very first emergence of an insurgent group, tasks such as indoctrination or combat training are of utmost importance, but gathering militants together may erode secrecy and bring risks. Although coordination and communication are necessary to organise a rebellion, the clandestine nature of the insurgency implies a trade-off. Modern communication technologies are changing this dynamic in favour of insurgents. They also provide effective means for in-group monitoring, which helps to overcome collective action problems such as free-riding. It is now easier for insurgent leaders to control militants across distant geographical locations, and there are channels to receive immediate feedback from militants in the field. The bidirectional flow of information between the upper and lower end of the hierarchy is now faster and has richer content, which leads to better decision-making processes and, therefore, effective operations.

I argue that the introduction of the 3G network in existing 2G network coverage areas facilitated a better communication medium for insurgents and improved their military operations, which translates into increased violence in a high-intensity episode of a civil war. I expect that the roll-out of the 3G network would lead to an increase in the number of violent events, IED attacks, and multiple coordinated attacks perpetrated by insurgents.

These arguments are tested with a disaggregated study of the war in Afghanistan, using the Open Cell ID dataset for information on network coverage and the Significant Activities (SIGACTs) dataset of the US Department of Defense for information on violent events (Shaver and Wright, 2016). Using matched wake analysis to alleviate the modifiable areal unit problem and selection bias (Schutte and Donnay, 2014), the results show that the introduction of 3G is linked to an increase in the number of attacks by insurgents in a variety of forms. The findings are confirmed with spatial regressions using the Global Terrorism Database (GTD) as an alternative source of information on violent events. The results are robust to a variety of specifications, different spatial unit sizes, placebo tests, and diagnostic tests for reporting bias.

The remainder of the chapter is organised as follows. I start with a brief review of the literature and then elaborate on my proposition by focusing on communications in an insurgent group and the potential benefits of advanced communication technologies for insurgents. I then elaborate on case selection and detail the datasets I use. Following the presentation of the research design and analysis, I conclude with a discussion of the findings.

3.2 A Brief Overview of the Literature

A growing body of literature has been seeking answers to how modern information and communication technologies (ICTs) shape conflict. Pierskalla and Hollenbach (2013) find that cell phone coverage increased the probability of violent conflict in Africa. Taking ethnic groups as the level of analysis, Bailard (2015) draws similar conclusions and proposes opportunities and motivations for conflict as explanations. On the other hand, using a military-sourced event dataset, Weidmann (2016) shows that cell phone coverage increases the likelihood of an event to be reported in the media, thus inducing bias to studies that rely on media-reported data. Shapiro and Weidmann (2015) finds that increased cell phone coverage in Iraq is associated with reduced insurgent violence, presumably due to increased information flow from

the population to the government.

These studies suggest that the effect of ICT on conflict may depend on the ability of actors to leverage the benefits of ICT. For governments to have the upper hand, the local population must be willing to share information about insurgents, and the technological capability of the government forces regarding signals intelligence and projection of force must be sufficient to suppress rebels. Shapiro and Siegel (2015) analyse this by assessing the relative gains of the conflict actors using a formal model. Proposing a theory in line with this approach and applying it to the context of terrorism, Mahmood and Jetter (2020) find a non-linear relationship in which terrorist events first increase as the amount of information flow increases in a country and then decrease with the further increase in information flow.

Some states exploit their control over the ICT infrastructure and the mass media. In a study of the Syrian conflict, Gohdes (2020) argues that states can provide Internet access selectively, depending on their intention to gain intelligence by tracking insurgent telecommunications and receiving tips from locals, or undermine insurgent activity and coordination by shutting down telecommunications. In a study of cell phone network shutdowns by the government of Pakistan, Mustafa (2023) finds that while the frequency of terrorist attacks tends to decline on days of shutdowns, it increases after shutdowns end. Similarly to modern ICT, the effects of mass media on conflict are likely to vary between contexts. Although radio broadcasts have been shown to have an effect on participation in killings in Rwandan genocide (Yanagizawa-Drott, 2014), Warren (2014) shows that the mass media infrastructure is associated with a lower probability of conflict in a study of 177 countries for the period between 1945-1999.

As a specific type of ICT, social media is also garnering attention. Warren (2015) demonstrate that higher levels of social media penetration are associated with an increase in violence in a subset of African states. Additionally, Zeitzoff (2018) finds that support on social media from public and international audiences can shift conflict intensity, suggesting that social media may exert an impact on the micro-dynamics of conflict. While political elites, gov-

ernment agencies, and rebel groups are increasingly using social media to communicate with the masses, social media platforms have also evolved into actors in contentious politics, with their policies and algorithms having significant implications that have yet to be explored (Zeitzoff, 2017). As conflict actors adapt to new communication mediums, we are likely to observe novel implications for conflict dynamics.

3.3 Modern Communication Technologies in Civil War

Regardless of the available technology, militants in a rebel group communicate for several purposes that are critical to the functioning and efficiency of the organisation. First, in terms of indoctrination, communication of the political cause and ideology to group members and to a wider audience is needed to gain support, mobilise locals, and radicalise militants. Second, combat training is essentially composed of conveying information on 'know-how' regarding topics such as the use of arms, preparing improvised explosive devices (IEDs), how to operate on the battlefield as a team and practising these collectively, which also requires communicating feedback. Communication is also crucial for monitoring members of a group, establishing control over militants, and making sure that all members contribute to the effort. A functioning command-and-control structure simply requires setting reliable means for communicating orders and directions from the leadership and receiving feedback from the members. Furthermore, having a suitable communication medium is essential to maintain real-time coordination between group members while conducting an attack, known as 'signal' communications. Finally, the insurgent leadership needs information from the militants in the field and from the local population to develop battlefield awareness and make informed operational decisions.

However, a fundamental problem that rebel groups face is ensuring their functioning, coordination, and collective action while remaining clandestine. Especially in the early stages of a civil conflict, when the rebel group is not strong enough to challenge the government,

militants must operate secretly to avoid being suppressed. This is manifested in cases where rebels are operating in small cells and minimising the contact between themselves. This trade-off sacrifices other complex tasks such as coordinating a sophisticated attack, or activities such as military training which sometimes requires facilities. As the group gradually grows in numbers and strength, they update their procedures considering risks and rewards for each course of action. New generations of communication technologies may offer a solution to this problem by facilitating exchange of information with richer content that is very close to face-to-face communication, without the need to gather militants together physically, further securing the organisation. This would make the vertical lines of communication 'thicker' in an organisation where otherwise the interaction between the smallest unit and its superiors is minimal.

While transitioning to more advanced communication technology may offer advantages to government forces, the specific benefits of shifting from 2G to 3G networks remain unclear. Unlike rebel groups, government forces do not face challenges in coordination and collective action while maintaining secrecy. They can gather for training or other purposes without compromising security, as they operate in large numbers and are located in fortified bases. Additionally, governments with signals intelligence capabilities can monitor communications within both 2G and 3G networks. Moreover, they often employ non-commercial technologies for within-group communication, which are designed to be as secure and encrypted as possible. While governments can use commercial communication technologies to receive tips from locals or cut down telecommunications to obscure rebel communications, the shift from 2G to 3G does not meaningfully alter these dynamics.

However, the adoption of new communication technologies and improved communication with richer content among militants can generate several advantages for a rebel group (Pierskalla and Hollenbach, 2013, pp. 210-211). In terms of indoctrination, these technologies can facilitate the rapid spread of a political cause or ideology, increasing group cohesion, while also undermining government propaganda. The spread of audiovisual content with narratives

can be more powerful than slogans or leaflets in 'winning hearts' of the populations. Tailored news from the battlefield, accompanied by propaganda materials, would keep sympathisers updated, aiming to maintain the momentum of popular support at the desired level. These efforts would contribute to the growth of the pool of potential recruits. Ideological education targets also militants, and it is now easier to provide militants with indoctrination material, regardless of how geographically dispersed they are. This would help maintain a high level of commitment throughout the conflict, especially when the rebel group is facing losses on the battlefield.

Modern ICTs can have a similarly positive effect on training. Even sophisticated knowledge, such as how to make IEDs, can be easily accessible to all members, thus 'democratising' expertise on technical issues. Unlike in the past, such 'skills' no longer require qualified personnel, such as militants with engineering education or military experience, nor do they necessitate the gathering of militants in a training camp. With detailed and clear instructions, complemented by images and videos, along with the possibility of receiving simultaneous help, it is now easier for an average militant to prepare an IED or carry out an attack with an off-the-shelf drone. As the weaker party in most conflicts, rebels need to innovate new tactics and methods. The availability of new communication technologies facilitates the quick and effective dissemination of such information and skills through clear guidelines, supported by audio and visual material.

Mobile communication can also be a tool for effective monitoring, helping to overcome free-riding problems by making sure that each member of the group and local supporters are contributing. It not only provides a medium to disseminate orders from the leadership to the militants, but also facilitates feedback from militants to the leadership. For example, verbal confirmation via radios used to be the standard method for rank-and-file militants to report to the upper echelons that a task is successfully done. In a setting where small units of militants are dispersed throughout a region, there were incentives to report 'fake' successes, where militants do not take risks of carrying out an attack while also appeasing the leadership.

However, new communication technologies facilitate more effective monitoring, as they make it practical for the leadership to ask for visual 'proof' to confirm such cases. Intensity of within-group communication can also increase trust between members and strengthen group networks, subsequently leading to a decrease in the number of defections from the group.

Moreover, ICTs enhance coordination among militants when conducting an operation. Given that they are often weaker than the government forces both in terms of quantity and quality, rebels must carefully plan and coordinate their movements and actions. This necessitates seamless communication within the group both during the planning process and the execution of the attack. Coordination among militant units is essential not only when multiple units are attacking a single target, but also when multiple units are attacking multiple targets simultaneously. The latter is especially preferable when feasible. Militants are well aware that government forces will retaliate after an attack. Moving reinforcements in response to an attack is one common reaction by counter-insurgents, not just with the aim of counter-attacking but also re-establishing the public order and helping the victims of the attack. Multiple simultaneous attacks would significantly reduce the risk of retaliation, by attacking the bases or routes of potential reinforcement forces from the neighbouring military units of the government. This would paralyse security forces and severely exacerbate their responses, and would provide militants a relatively safer way to retreat to more secure locations. Furthermore, multiple simultaneous attacks are a much stronger way of signalling, showcasing the rebels' strength and capabilities while exposing the weaknesses and vulnerabilities of the incumbent forces. Such coordinated attacks may induce chaos and panic among security forces and the population, causing delays in providing help and reinforcement and undermining public trust in the government.

Finally, new technologies may increase the quality of information that rebel groups receive from local informants, active supporters, and local militias. Except for accidental engagements between militants and government forces, attacks carried out by rebel groups are often planned for a relatively long time, supported by a continuous effort of reconnaissance aided

by auxiliary forces and informants. Typically, these efforts aim to obtain very detailed information about targets, such as the exact positions of trenches or the routine schedules of guard rotations in a military base. Local informants are also a resource of information on the activities of government forces, acting as an early warning system to secure militants. While such information can also be received by other means, new technologies would make it quicker with richer content. The potential uses of modern ICTs by rebels and their implications discussed so far are summarised in Table 3.1.

Areas of ICT usage	**Implications**
Indoctrination and propaganda	Increase in recruitment, increase in the commitment of militants
Training and know-how	Increase in attacks, particularly with innovative tactics such as IEDs or drones
In-group monitoring	Decrease in defection, decrease in free-riding
Real-time coordination (Signals communication)	Increase in the number of coordinated complex attacks
Intelligence and battlefield awareness	Increase in overall effectiveness (Increase in attacks during a high intensity episode of conflict) Decrease in losses

Table 3.1: Insurgent use of ICT and their implications

The predecessors of modern technologies not only allowed for limited content, but were also less effective compared to today. For example, radio communications had been the primary medium of communication within the combatants, but they were very vulnerable to interception by the governments. Encrypting these communications was not possible for most rebel groups, and they were compelled to use primitive types of encoding, which decreases efficiency and increases the time needed to convey a message. Although new communication technologies may also be vulnerable to interception by states which have advanced capabilities of signals intelligence, secure communications are more accessible than before, thanks to new cloud-based instant messaging applications. Furthermore, rebel groups would find 3G mobile networks (and subsequent generations) more practically advantageous than fixed broadband

internet, as it allows militants to remain 'mobile' while staying connected.

While each implication in Table 3.1 warrants empirical examination, some of them present practical challenges in observation. Reliable and precise information on the recruitment and total size of rebel groups is not available for most civil wars. Similarly, data on defections are often sensitive and are not typically disclosed by governments. Other implications can only be observed from within the group, such as the level of commitment among militants or the presence of free-riding behaviour. However, it is important to recognise that these implications are interconnected and operate within a broader context, contributing to the accomplishment of an overarching strategic objective for the group. For a rebel group fighting an intense civil war, the desired outcome is conducting successful attacks, keeping the momentum, and keeping the growth of the organisation by increasing recruitment while minimising losses.

Successful offensives by the rebels should be manifested in the number of violent attacks, rather than the number of inflicted casualties or suffered losses. While better planning and collective action should mean that rebels lose fewer militants in their attacks, not all clashes –and therefore casualties– are planned by the rebels. On many occasions, clashes between rebels and government forces can occur with the initiative of the latter. Second, the number of casualties perpetrated is also a function of the government's capacity to protect themselves and the local population. Third, not all rebel attacks are meant to inflict as many casualties as possible. A specific target may be of higher importance to the rebel group, sometimes even non-lethal targets such as infrastructure. Finally, better communication would increase the speed and success of decision making and planning, which translates into a higher number of attacks.

H1: The introduction of 3G network coverage increases the number of attacks by rebel groups compared to areas with 2G network coverage.

The increase in the number of attacks is an overarching outcome in which all discussed mechanisms can be in play during a high-intensity intrastate war. However, some mechanisms may also result in an increase in specific types of violence. The dissemination of information between militants on know-how would increase the use of innovative tactics such as IED attacks. The logistics and execution of such attacks are typically planned in fine detail, and this would benefit from better intelligence and battlefield awareness. Advanced communication technologies can accelerate the learning process, facilitate operations, and allow a larger number of militants to execute IED attacks.

H2: The introduction of 3G network coverage increases the number of IED attacks by rebel groups compared to areas with 2G network coverage.

Finally, advanced communication technologies facilitate a rapid flow of information with richer content within the organisation, both vertically and horizontally. This improvement in information processing can reduce communication costs and enable militant leadership to command larger-scale operations throughout their area of presence. Simultaneous attacks across multiple locations may be preferred for several reasons, including greater impact and stronger signaling. However, the execution of such attacks requires detailed planning and an open line of communication between militant units during the operation. If new generations of communication technologies improve intelligence gathering and 'signals' communication, we should observe an increase in the number of multiple coordinated attacks.

H3: The introduction of 3G network coverage increases the number of coordinated multiple attacks by rebel groups compared to areas with 2G network coverage.

3.4 War and Telecommunications in Afghanistan

The case of Afghanistan presents a tough test for the proposed arguments. The United States and allies had a strong presence supporting the Afghan government in the fight against insurgents. They had significantly high capacity to capitalise on the communication network and gather intelligence by detection of telecommunication signals, accompanied by the capability of precision targeting. This makes using any means of mobile communication risky for Afghan insurgents, potentially offsetting benefits. Taliban is one of the rebel groups that attacked telecommunication infrastructure most, probably over concerns of being detected and targeted. Besides, although they do have presence in cities, the insurgency is rather rural-based, while the communication network is more likely to be clustered in major cities and roads.

Afghan insurgents have a multifaceted relationship with technology. As the Taliban's infamous ban on television and media before the international intervention in 2001 consolidated the anti-modern image, it was surprising to many that they are utilising telecommunication technology for their propaganda efforts. Taliban embraced technology to disseminate propaganda from the early years of the war (Giustozzi, 2007). Since the mid 2000s, they have a strong presence in the virtual world, with websites in different languages (Sediqi and Jain, 2019), social media accounts (Mozur, 2021), channels on cloud-based messaging applications (Meek, 2015), and two official spokespersons (Bashir, 2017). They even attempted to launch a mobile application on the 'Google Play Store' in 2016, however it was removed from the platform immediately (BBC, 2016). Their messages consist mainly of news from the battlefield, supported by images, videos, and propaganda material such as religious chants. Their efforts to make use of the internet and social media have recently received international attention as they try to re-brand themselves with the end of the two-decade long conflict (Kann, 2021; Mozur, 2021; Saeed, 2021). Besides Taliban, the Islamic State, which has an offshoot group in Afghanistan, is also well-known for effectively using the internet and social media

for its propaganda efforts.

While it is evident that insurgents have been utilising telecommunications for propaganda and recruitment purposes, it is difficult to observe the extent they leverage technology for within-group communication and coordination throughout the conflict. As early as 2003, Taliban was investing in motorcycle reconnaissance scout teams with satellite phones, and using radios to coordinate militants on the battlefield (Giustozzi, 2007, p. 152). Videos from the battlefield in their propaganda material is also another indicator, which in later periods showed that militants do use 'smartphones.' Another notable indicator was the use of IEDs triggered by cell phone signals (Ankersen and Martin, 2021). However, the Taliban's utilisation of telecommunications was selective, primarily using it when it offered advantages. During offensives by the US and its allies, they became vulnerable to detection and targeting, through signals intelligence and tips from the local population. Consequently, the Taliban resorted to attacking the telecommunication infrastructure on multiple occasions and exerted pressure on mobile network companies to deactivate their cell phone towers during specific periods of the day (BBC, 2012). Nevertheless, a questionnaire made in 2012 among 38 Taliban commanders in Helmand province shows that about 80% of them did not believe that their use of cell phones cause them to be detected and targeted by counter-insurgents (Giustozzi, 2019, pp. 150-151). Concerns over insecurity of telecommunications were even less pronounced after the withdrawal of the International Security Assistance Force (ISAF) in December 2014 (Giustozzi, 2019, p. 151). It has been reported that both the Taliban and the Afghan government were too reliant on the *WhatsApp*, after the instant messaging application became widespread in the country. The insurgents considered it an effective medium for within group communications and coordination, with the speed and flexibility it provides, as well as the voice message feature which allows illiterate militants to use it (Gibbons-neff and Mashal, 2019). This reliance still continues after the Taliban takeover in 2021, and although users linked to the Taliban are occasionally removed from the platform, militants are circumventing these measures by acquiring new SIM cards and opening new

accounts (Goldbaum and Padshah, 2023).

However, the telecommunications sector emerged as one of the most remarkable success stories in the Afghan economy. Prior to 2001, the country had fewer than 15000 local landlines, no international calling facilities, no internet connectivity, and no ICT institutions and companies (Payab, 2009). Soon after the toppling of the Taliban from power, successful policies regulating ICT were introduced and the industry started to flourish. As the sector was shown to be profitable with the first two companies (Afghan Wireless Communication Company and Roshan), three more actors joined the competition (MTN, Etisalat, and Salaam), bringing investments in telecommunication infrastructure. According to the International Telecommunications Union (ITU), mobile subscriptions per 100 inhabitants increased from 35 in 2010 to 58 in 2020, and approximately 90% of the population were covered by at least 2G network in 2020. Introduced to country in 2013, and the population covered by the 3G network gradually expanded to 57% in 2020. In contrast, fixed broadband internet subscriptions remained low, reaching only 7% of the population in 2020. This makes the impact of mobile broadband more relevant in the case of Afghanistan, as it represents the majority of internet usage. The proportion of the population covered by the 4G network has also reached 26% since its launch in 2017 (ITU, no date). The use of smartphones and social media is widespread, especially among the younger population. The evolution of the coverage of the 2G and 3G networks over time is visualised in Figure 3.1, using the Open Cell ID database.

The success story of mobile telecommunication companies was not without challenges, particularly in rural areas with insurgent influence and control. These companies faced a difficult situation, caught between the demands of the Afghan government and the threats posed by the Taliban. Afghan government pressured the companies to expand their network in areas under insurgent influence and control, considering that it would facilitate denouncing of insurgents by the local population. Taliban, on the other hand, threatened companies to attack their infrastructure and personnel, if they do not obey the restrictions requested by them. Although the Taliban did not reject the expansion of the network in their areas of

control, they forced companies to switch off their cell phone towers at certain times of the day. As they are essentially a complex network of segmented groups, there was variation between regions, but most commonly the network was asked to be turned off at night. As the Taliban increased its influence and control, it started to tax companies, and companies complied since it was the only way to continue operating in these areas. The lack of control on companies by the Afghan government might also indicate that it was less likely to receive information on insurgent activity from companies. Additionally, Salaam, a company associated with the Afghan government, was not allowed to operate in areas under Taliban control, and local people using Salaam sim cards were often taken their sim cards off and beaten at Taliban checkpoints (Clark, 2020). Later, the Taliban began taxing local residents on their cellular subscriptions in some regions, and mobile companies even paid the Taliban for protection of their personnel and infrastructure (Clark and Bjelica, 2018). In an interview with the Taliban's head of 'Control and Coordination Commission for Non-governmental Organisations and Companies,' published by Taliban on 20 March 2014, it was emphasised that the commission was responsible for overseeing the telecommunication network, that the temporary network closures were subject to the demands of both 'the masses' and 'the mujahedeen,' and that the Taliban provided assistance to telecommunication companies for security and transportation of their personnel and equipment (Strick van Linschoten and Kuehn, 2018, p. 464).

3.5 Data and Research Design

3.5.1 Dependent Variable

For data on violent events, I use the Significant Activities (SIGACTs) dataset of the US Defense Department for Operation Enduring Freedom (Shaver and Wright, 2016).[2] The

[2]I am thankful to Andrew C. Shaver and Austin L. Wright for sharing this dataset. See Shaver and Wright (2016) for a complete description of the data.

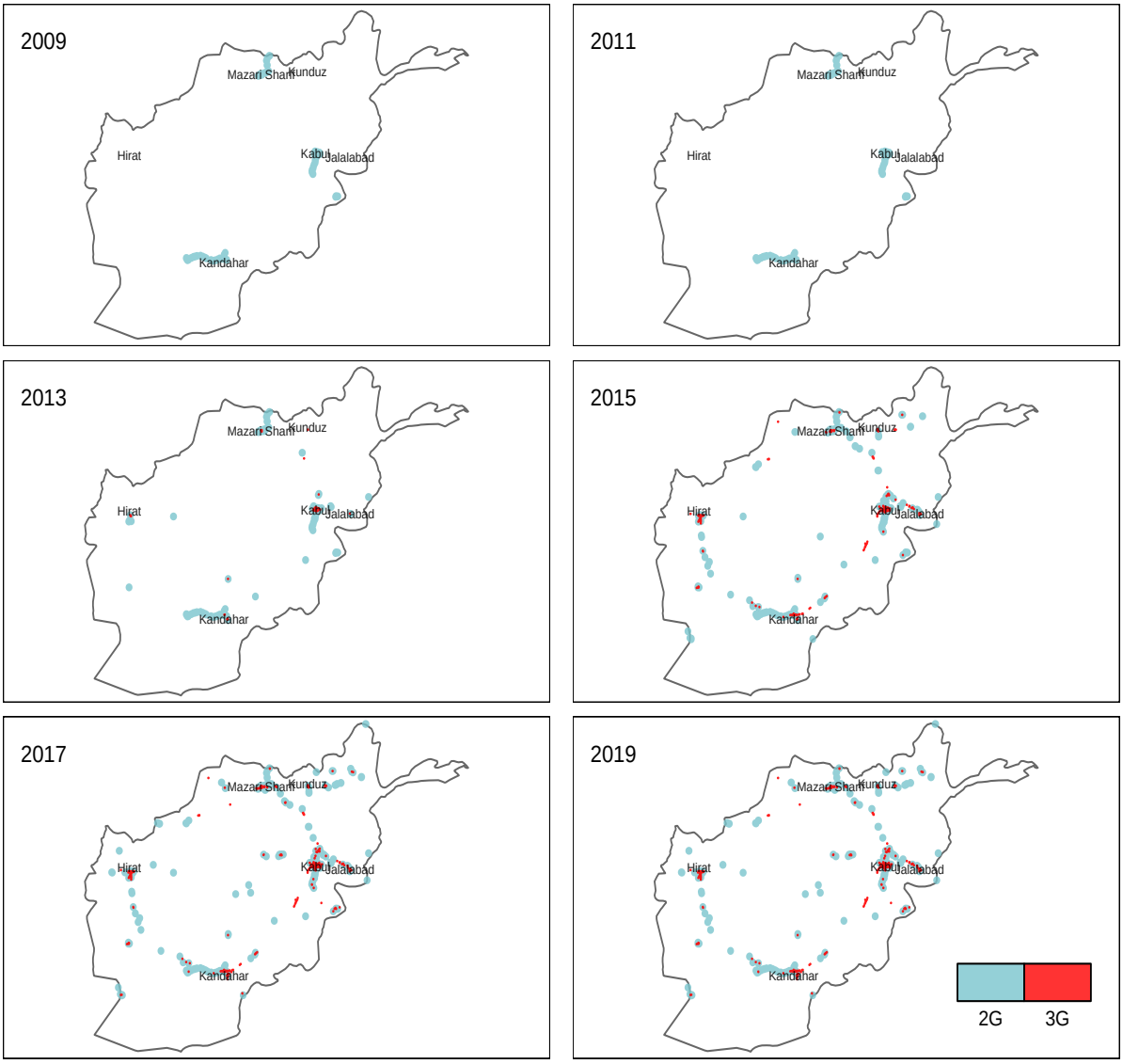


Figure 3.1: Evolution of Mobile Network Coverage in Afghanistan
(Source: Open Cell ID Project)

SIGACTs dataset has several remarkable advantages over media-based conflict event data, in particular for micro-level study of violence over space and time. The dataset covers a variety of event types related to the conflict and to the counter-insurgency efforts. For this study, I focus on insurgent-initiated violent events including direct and indirect fire as well as IED attacks.[3] A limitation of the SIGACTs dataset is that the temporal coverage is up until the end of 2014, which limits the leverage of the network data available.[4] Between 2010 and 2014, the dataset covers 174145 insurgent-initiated violent events.

The SIGACTs dataset provides a more complete picture of the conflict and is less likely to be biased compared to media-based event datasets. It was originally coded by military personnel for evaluation and planning purposes. Not being coded for public reporting alleviates selection biases over newsworthiness or political concerns, unlike news media. Another important advantage of the SIGACTs lies in its precise geo-coding. Event locations are coded by military personnel, mostly using GPS devices and the military grid reference coordinate system. These are almost precise locations, as the internal standards in terms of accuracy are high in the military, due to the use of this information in planning and evaluation. For example, having a complete account of previous events can help military commanders plan a safe route for a convoy, avoiding potential ambush locations. This is more important in a setting where military personnel are deployed for short periods, to keep an institutional memory for the benefit of future deployments.

For testing *H3*, I focus on multiple coordinated attacks, which is a direct indicator of the capabilities regarding coordination and collective action. While individual attacks may increase or decrease for various reasons in different episodes of conflict, an increase in multiple simultaneous attacks suggests a clear improvement in coordination. Here, I use the Global Terrorism Database (GTD), focusing on events that are coded as *part of multiple incident*. This variable indicates cases where several attacks are connected, and where either time or

[3]Event types in the data are coded as 'Enemy Action', 'Explosive Hazard' and 'Friendly Action.' While I focus on the first two categories for the main analyses, I use the latter category as a robustness check.

[4]While 3G was introduced in Afghanistan in 2013, 2015 and afterwards saw a major roll-out of the network.

locations of these incidents are discontinuous so that they cannot be considered as a single attack in the coding process. The concerns about using media-based event datasets are less problematic in case of multiple coordinated attacks, as they typically have substantial impacts and are less likely to be missed by the news media. Weidmann (2016, pp. 215-216) shows that as the severity of a violent event increases, the reporting bias tends to diminish. In a similar vein, multiple attacks can be perceived as significant akin to an individual incident with high severity.

3.5.2 Independent Variable

I use the Open Cell ID database for information on the locations of the 2G and 3G network towers. Open Cell ID is an open source project which uses several mobile phone applications to collect information on the locations of cell phone towers, with first and last dates of observation. Although this makes data clustered in settlement areas and roads, the Open Cell ID project offers a more reliable and impartial source of data. Commercial companies may have incentives to exaggerate their coverage areas, and they are often reluctant to share data as they compete with each other within the same country and treat such information as confidential. Additionally, the Open Cell ID project offers the advantage of building a time series that tracks network expansion by using the dates of first observation. I assume that militants (and local informants of rebels) would use 3G technology when it is available. From the accounts depicting the group and the conflict, it is likely that at least a few militants use it in each unit of militants operating together.

The temporal coverage of Open Cell ID data for the network in Afghanistan starts from 2009. However, the first observations of towers from this year likely represent the existing network at that time, which may not accurately reflect the true timing of tower installations. Therefore, I focus on observations dated from 2010 onwards until the end of the SIGACTs data coverage in 2014. Throughout this period, there were 339 2G towers and 165 3G towers installed, with the introduction of 3G beginning in 2013.

3.5.3 Research Design

Matched Wake Analysis

I employ *matched wake analysis*, to investigate the relationship between the 3G network and violent events, taking the 2G network as the control group (Schutte and Donnay, 2014). Matched wake analysis (MWA) uses sliding spatio-temporal windows of varying sizes to overcome 'modifiable areal unit problem' (MAUP) and coarsened exact matching (Iacus, King and Porro, 2012) to increase covariate balance between treatment and control units. Here, the instalment of a 3G network tower is considered a treatment event, while the instalments of 2G towers are control events. Buffer zones are generated around the locations of treatment and control events, setting up the spatial unit of analysis. These spatial units are then extended t time unit before and after the timing of treatment and control events, resulting in spatio-temporal 'cylinders' for each treatment and control intervention. In order to increase balance between the treatment and the control group, spatio-temporal cylinders are matched on pre-trends in violent events, pre-exposure to control and treatment, and covariates that are likely to be confounders. Matching on pre-trends in violent events is done by dividing the 'pre-' half of the spatio-temporal cylinder into two and calculating a temporal trend over the subsequent two pre-periods (Schutte and Donnay, 2014, p. 3). Matching units with similar treatment and control history is a remedy to alleviate the violation of the 'stable unit treatment value assumption' (SUTVA), since there are overlaps of treatment and control events in the data (Schutte and Donnay, 2014, pp. 4-6). Using the resulting sample from the matching process, the pre- and post-spatiotemporal windows are compared by counting the number of violent events for each window, then applying a 2×2 difference-in-differences regression. The same process is replicated with different spatial and temporal unit sizes, and resulting estimates for each unit size are presented.

Several factors make MWA favourable for the setup in this study. Since the 3G network will be compared to the 2G network, rather than out-of-network areas, we have control

events rather than untreated units as the control group. Second, rerunning the analysis using varying sizes of spatial and temporal units increases confidence in the findings that they are not driven by the selection of the spatial and temporal unit size (Cook and Weidmann, 2021). Varying spatial unit sizes also allow us to assess how far the effects of the treatment reach spatially. Using arbitrary unit sizes in analyses requires high geo-coding precision in the data, which SIGACTs dataset meets. Third, the above-mentioned matching process helps alleviate the imbalance between the treatment and control groups, and it remedies the violation of SUTVA.

However, it is difficult to make a causal claim in this study, even though the matched wake analysis is designed for causal inference. On the one hand, since the 3G network is almost always introduced in areas where the 2G network is already present, 2G network areas should be more likely to exhibit similar characteristics with areas where the 3G is introduced, such as population or income, compared to areas outside the network. On the other hand, the rollout of 2G and 3G networks is not random. They start in the capital and in large urban areas, and then gradually grow to cover other towns and settlements. In the case of Afghanistan, there are indicators that the rollout was demand driven and companies tried to resist the effect of conflict on their businesses. The growth of the telecommunications sector is likely to be encouraged by the government and allies, as it was the engine of the economy. Even when a cell phone tower was destroyed by the insurgents, it was quickly replaced by the companies. Taliban spared companies that obeyed their demands, sometimes had to compromise with local populations who demand network access, and in some cases benefited from the tax revenue. Cities and roads, where the network is clustered, often experienced violent events, but the network continued to grow.

For matching, I use several covariates that are likely to affect both the network roll-out and violence. Population can increase the demand for the cell phone network, while studies also show a positive relationship between the size of the local population and the number of violent events in conflict contexts (Raleigh and Hegre, 2009). To take this into account,

I use population data from CIESIN (2018). Another factor that may affect infrastructure demand is the income and level of local development, which may be negatively correlated with violence. To proxy for this effect, I used stable nighttime lights data from the National Oceanic and Atmospheric Administration (NOAA, no date). Similarly, rough and inaccessible terrain may provide shelter for insurgents (Buhaug, Gates and Lujala, 2009; Fearon and Laitin, 2003), while network build-up can be logistically difficult in such areas. To account for this, I use data on elevation above sea level from Gesch, Verdin and Greenlee (1999). All three sources of information are geo-coded at the level of 30 arc-second (approximately 1 km at the equator) resolution cells, and values are assigned to treatment and control observations using the geo-locations of towers. Finally, to account for the remoteness of the tower locations, I coded the distances to the nearest provincial capital for each tower.

When generating its coverage data, the GSM Association (GMSA) considers the coverage radius of a 3G cell tower to be 4 km and a 2G cell tower to be 12 km. It bases these numbers on the information provided by operators, with a tendency towards minimum values. Therefore, I specify spatial unit sizes starting from 4 km radius, up to 20 km, and increasing it by 4 km in each step. Temporal intervals vary from 30 to 90 days by 15-day increases each time, considering that the expected effects of 3G discussed above are not immediate effects. For each combination of spatial and temporal resolution, the number of dependent events (insurgent initiated violent events for *H1* and IED attacks for *H2*) is counted for each spatio-temporal window, and the pre-control and pre-treatment windows are matched on covariates, pre-exposure to treatment and control, and pre-trends in dependent events. The difference-in-differences specification below is run using the resulting sample for each spatio-temporal unit specification, and the estimates for the quantity of interest, β_{3G}, are presented.

$$n_{post} = \beta_0 + \beta_1 n_{pre} + \beta_{3G}\text{treatment} + u \tag{3.1}$$

Spatial Regression

Since GTD is used for identifying coordinated attacks to test *H3*, I move to a spatial regression design considering the geo-approximations in the coding process.[5] I built a balanced time series cross-sectional dataset using secondary-level administrative units (Wuleswali) and quarters as the spatial and temporal units of analysis. Around the geo-locations of cell phone towers, buffer zones were created that represent coverage. Following GSMA, I set the radius for each buffer at 4 km for 3G towers and 12 km for 2G towers.[6] Using these buffer zones, I created a time series of network coverage by quarter. I then calculated the proportion of each spatial unit covered by each network.[7]

To estimate the effects of the 3G network, I utilise a two-way fixed effects model that accounts for spatial dependencies. Both network coverage and conflict events are spatial phenomena that are likely to cluster, implying spatial interdependencies. Network infrastructure is likely to be clustered around urban areas and main roads, and they may have spillover effects where an effect in a certain location may realise in a neighbouring location, since militants can move to neighbouring locations quickly. Unobserved predictors of violence may also be spatially dependent. In addition, locations that experience violent events might attract infrastructure if the government considers it as a means to receive tips and information from the local population. Therefore, to rule out temporal and spatial dependencies and address simultaneity concerns, I use several lagged variables in the model. I temporally lag the 2G and 3G network coverage variables for one quarter. A contemporaneous spatial lag of the outcome to control for spillovers in violent events and a spatial error term to account for spa-

[5]Event locations in GTD are coded using the coordinates of the centres of city, village or town that the event occurred, or the centroid of the smallest administrative region can be identified (START, 2021, pp. 23-24).

[6]This approach does not account for variations in terrain, but I consider this to be of minor significance for two reasons. First, telecommunication companies typically choose the most suitable locations for cell phone towers to maximise coverage, thereby reducing potential errors in this approach. Second, the buffer zones used in this study are not large enough to encompass geographic features that could significantly impact signal reach.

[7]I consider this approach as more informative than a binary variable (i.e. setting an arbitrary threshold and coding the network coverage as 1 for values above that level) since the geographical sizes of the secondary level administrative units are much larger than the coverage areas of the individual towers.

tial dependency in unobservables are also added to the model, along with spatial lags of 2G and 3G coverage variables. I model spatial connectivity between units with a row-normalised first-order queen contiguity matrix, where administrative units sharing borders are identified as neighbours. The resulting model can be formalised as;

$$y_{i,t} = \alpha_i + \alpha_t + \rho \mathbf{w}_i \mathbf{y}_t + \theta_{2G} \mathbf{w}_i \mathbf{2G}_t + \theta_{3G} \mathbf{w}_i \mathbf{3G}_t + \beta_{2G} 2G_{i,t-1} + \beta_{3G} 3G_{i,t-1} + u_{i,t} \qquad (3.2)$$

$$\text{where, } u_{i,t} = \lambda \mathbf{w}_i \mathbf{u}_t + \varepsilon_{i,t},$$

where α_i and α_t are unit and time fixed effects, ρ is the coefficient of the spatial lag of the outcome y, θ_{2G} and θ_{3G} are the coefficients of spatial lags of the 2G and 3G network variables, λ is the coefficient of spatial error term, $\mathbf{w}_i$ is the vector of unit i's connectivity to other units. Here, the quantities of interest are β_{2G} and β_{3G}, and the priority is to remove all potential dependencies rather than to model and estimate specific dependencies. Therefore, an adjusted version of the spatial general nesting model is used. As it is proposed that the effect of the 3G network is greater compared to 2G, the following hypothesis test will be conducted: $H_0 : \beta_{3G} - \beta_{2G} \leq 0$.

3.6 Results

3.6.1 Matched Wake Analysis

Matched wake analysis is conducted using temporal resolutions ranging from one month to three months, and spatial resolutions from 4 km, which represents the average coverage radius of a 3G network tower, to 20 km. The results show clear patterns of an increase in overall rebel violence with the introduction of 3G coverage. Estimates with varying sizes of spatio-temporal units are predominantly positive and statistically significant, within a range of spatial and temporal distances from the locations of treatment, i.e., 3G towers. For instance, on average, an instalment of a 3G tower is associated with an increase in the number of

attacks by about 7 within a 8 km-wide region in a 75-day period, compared to an instalment of a 2G tower. The estimated coefficient varies from 1.74 in the smallest spatio-temporal unit to 7.66 for the largest estimate, within a 16 km range in a 90-day period. The relationship is even stronger in the case of IED attacks, with almost all estimated coefficients being positive and statistically significant. For example, on average, there is an increase of 5 IED attacks within a spatio-temporal unit of 20 km $\times$ 60 days, compared to the control units.[8] Overall, there is strong support for both hypotheses.

The results are summarised in the contour plots in Figure 3.2, showing the estimates of β_{3G} from the difference-in-differences regressions. All non-shaded areas show statistically significant estimates at $p < 0.05$ level. The areas with dotted lines show estimates with p values between 0.05 and 0.1, and the areas with solid lines show statistically insignificant estimates. Detailed results from combinations of temporal and spatial window sizes with significant estimates are presented in Table 3.2, with estimated coefficient sizes and p-values for these combinations.[9] Improvement in balance after matching is also presented, showing the *L1* imbalance measure and the percentage of common support (Iacus, King and Porro, 2012). An overall improvement in these measures is present in the post-matching samples. Overlaps in the resulting sample are also presented, with 'same overlap' (SO) referring to two or more occurrences of the same type of intervention in a spatio-temporal window, while 'mixed overlap' (MO) referring to the cases where treatment and control events overlap in the same unit of space-time. Although these cases imply violations of SUTVA, note that the matching on treatment and control event history is used as a remedy for this problem (Schutte and Donnay, 2014, p. 4). Monte Carlo simulations show that increasing the percentage of overlaps increases standard errors, but the point estimates remain accurate (Schutte and

[8]Some types of IEDs are designed to be triggered by cell phone signals by the perpetrator, so they are by nature observed in coverage areas. Note that, however, 2G coverage is enough for this, and since the comparison is between 2G and 3G, it should not affect the results. Furthermore, from a tactical point of view, IEDs are more likely to be detonated on convoy routes outside urban centres, preferably with geographical features for the perpetrator to hide and without alternative routes for the targeted convoy, which are more likely to be 2G network areas than 3G.

[9]Detailed results for the IED attacks as the outcome are presented in Appendix 3.A.

Donnay, 2014, p. 6).

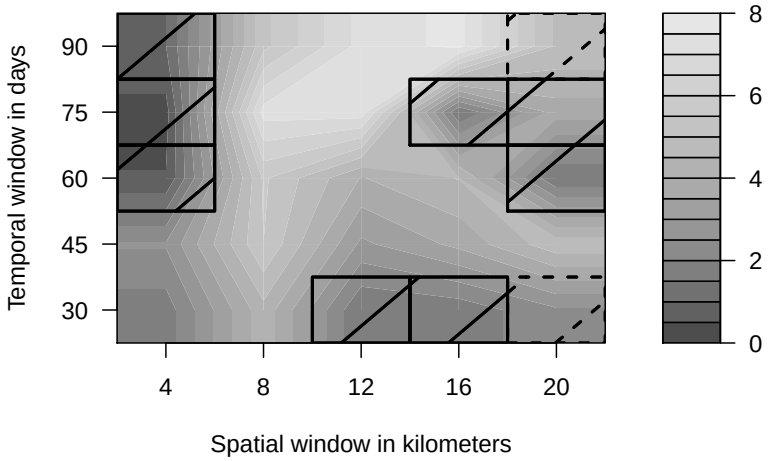
3.6.2 Spatial Regression

To test *H3*, I use a balanced panel dataset of districts (N = 398) in Afghanistan over a longer time period of 42 quarters from 2009 to the end of 2019, exploiting the greater temporal coverage of the GTD dataset. The dependent variable of *H3* is the number of multiple coordinated attacks, which I extracted from the GTD dataset using the *multiple incident* indicator. The results are presented in Table 3.3, which provide strong support in favour of the hypothesis.[10] I start with a simple two–way fixed effects model (Model 1), which shows a large contrast between the coefficients of 2G and 3G network coverage variables in both direction and magnitude. In Model 2, instead of time and unit fixed effects, I specify a spatial general nesting model with a time lag of the dependent variable, expecting to rule out potential spatial and temporal dependencies. Among those extra parameters, the spatial lag and the time lag of the outcome are positive and statistically significant, while the spatial error term is negative and statistically significant. The coefficient of the 3G network is still statistically significant and substantively larger than the 2G network. I move to the main specification in Model 3 by including spatial terms and two–way fixed effects.[11] The coefficients are closer to Model 1 in terms of direction, significance, and magnitude, demonstrating that the 3G network has a much more profound association with multiple coordinated attacks compared to the 2G network. In all models, the coefficient for the 2G network is indistinguishable from zero. All p values to reject the null hypothesis of $H_0 : \beta_{3G} - \beta_{2G} \leq 0$ are above the conventional levels of statistical significance, and the t values for this hypothesis test are presented in the corresponding row in Table 3.3.[12]

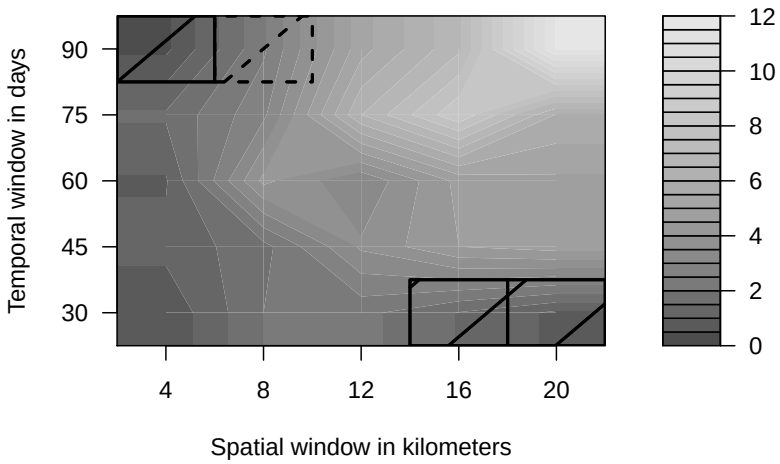
[10] I replicate spatial regression analyses to test *H1* and *H2* using GTD, to demonstrate that the findings supporting both hypotheses hold when the GTD is used. The results are similar to Table 3.3, providing additional evidence in support of *H1* and *H2* (see Appendix 3.B).

[11] I do not include time lag of the outcome together with time fixed effects, as it would generate inconsistent estimates (Nickell, 1981).

[12] However, interpretation of effects should be made cautiously, as we do not certainly know that the probabilities of reporting between the two networks are similar. To further increase confidence in the results, I perform a diagnosis test based on a potential implication of the existence of reporting bias, following



(a) DV: N. of Rebel Attacks



(b) DV: N. of IED Attacks

Contour plots showing the treatment effect estimates from the difference-in-differences regression, with 2G as the control and 3G as the treatment group. The dependent variable is the number of violent events by insurgents for the above plot, and the number of IED attacks by insurgents for the below plot. In the clear areas, the estimate is significant at .05 level. Dotted areas are significant at 0.1, and in areas with solid lines, the estimate is insignificant. Note that the estimates are predominantly positive and significant in both plots. The plots are generated using `mwa` package in `R` (Schutte and Donnay, 2014).

Figure 3.2: Empirical results of matched wake analysis

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	30.00	4.00	1.74	0.00	0.28	339	157	0.88	8.00	0.77	0.14	69	90	0.76	18.00	0.51	0.29
2	30.00	8.00	4.33	0.00	0.25	339	157	0.95	3.70	0.82	0.23	57	72	0.76	16.50	0.60	0.44
3	45.00	4.00	2.55	0.00	0.33	339	157	0.90	7.70	0.78	0.15	72	88	0.83	13.50	0.54	0.31
4	45.00	8.00	5.50	0.00	0.33	339	157	0.94	4.70	0.84	0.26	56	92	0.93	6.60	0.65	0.46
5	45.00	12.00	2.89	0.01	0.51	339	157	0.94	4.70	0.86	0.30	70	71	0.93	4.30	0.73	0.54
6	45.00	16.00	3.64	0.00	0.57	339	157	0.94	4.40	0.87	0.32	70	67	0.93	5.70	0.75	0.55
7	45.00	20.00	4.84	0.00	0.50	339	157	0.95	3.20	0.87	0.32	56	61	0.93	5.40	0.75	0.57
8	60.00	8.00	5.58	0.00	0.44	339	157	0.96	3.60	0.86	0.27	55	87	0.85	13.80	0.68	0.48
9	60.00	12.00	3.97	0.00	0.56	339	157	0.96	2.80	0.88	0.31	77	75	0.94	5.10	0.75	0.55
10	60.00	16.00	4.53	0.01	0.55	339	157	0.93	4.60	0.88	0.32	52	70	0.93	4.90	0.77	0.57
11	75.00	8.00	7.22	0.00	0.57	337	146	0.96	3.00	0.87	0.30	57	82	0.85	9.20	0.70	0.52
12	75.00	12.00	7.30	0.00	0.60	337	146	0.97	2.20	0.89	0.32	67	58	0.94	3.90	0.76	0.58
13	90.00	8.00	5.36	0.00	0.47	336	146	0.95	3.30	0.88	0.37	82	91	0.92	5.30	0.74	0.56
14	90.00	12.00	7.18	0.00	0.43	336	146	0.97	2.10	0.89	0.40	56	69	0.97	2.70	0.77	0.62
15	90.00	16.00	7.66	0.02	0.41	336	146	0.96	2.50	0.90	0.40	50	50	0.92	4.60	0.79	0.62

Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and right-hand side, respectively. The *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

Table 3.2: Overview of the Matched Wake Analysis Results

	DV: N. of Coordinated Attacks (*log*)		
	Model 1	Model 2	Model 3
Intercept		0.016^{***}	
		(0.002)	
2G Coverage$_{t-1}$	−0.033	0.004	−0.029
	(0.021)	(0.018)	(0.027)
3G Coverage$_{t-1}$	0.145^{***}	0.287^{***}	0.195^{***}
	(0.037)	(0.042)	(0.050)
log Attacks$_{t-1}$		0.161^{***}	
		(0.006)	
Spatial terms[†]		✓	✓
District (Wuleswali) FE	✓		✓
Quarter-year FE	✓		✓
$t_{\beta_{3G}>\beta_{2G}}$	3.758	5.279	3.540
AIC	3606.484	4033.256	65900.88
Log Likelihood	−1361.242	−2010.628	−32504.44

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$. Standard errors are in parentheses.

[†] Spatial terms include coefficients for the spatial lag of dependent variable (ρ), spatial lags of 2G and 3G coverage (θ_{2G}, θ_{3G}), and the spatial error parameter (λ).

A balanced panel dataset with 16716 observations (398 districts × 42 quarters) is used in all models.

Table 3.3: Regressions on multiple coordinated attacks

3.6.3 Placebo Tests

While the results provide strong evidence in favour of the hypotheses, it is important to note that the roll-out of both 2G and 3G network infrastructure is not random, and the networks tend to cluster in urban areas and along major roads. If other factors were affecting both levels of violence and selection into treatment, findings may be spurious. To address concerns over selection bias, I use placebo tests to confirm that there are no effects of future 3G network installations on present violence. I replicate the matched wake analyses for *H1* and *H2* by changing the treatment time to 3 months and 6 months before the true timing of the treatment. Note that the comparison is still with the 2G network areas, which are all

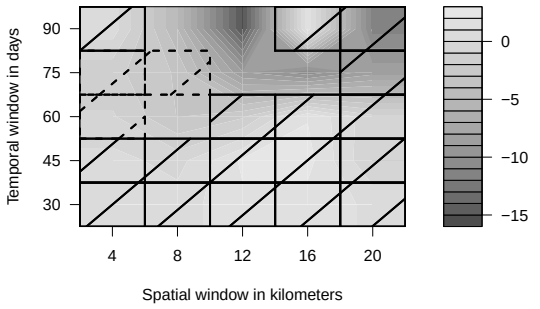
Weidmann (2016). The results suggest that there might be an increase in the probability of reporting in areas of the 3G network compared to 2G for less severe events. As the severity of the event increases, this trend quickly diminishes and the potential bias is not strong enough to overturn the results (see Appendix 3.C).

potential future recipients of treatment, by upgrading to the 3G network. Areas out of 2G coverage are less likely to receive treatment in the future and are not included in the analyses. Finding evidence of positive effects for future treatments would imply that the results may be driven by other factors that also affect the selection into treatment.

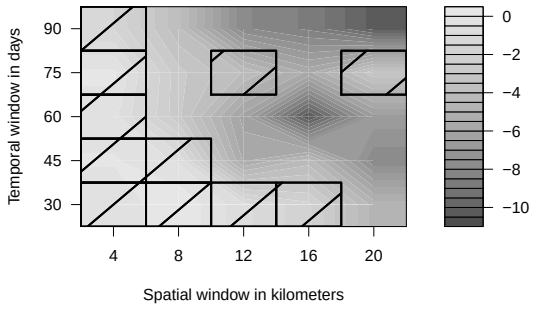
The results of the placebo tests show substantial and profound changes. For future treatments offsetting 3 months before the true treatment timing, most of the combinations of spatio-temporal units yield statistically insignificant results, and all significant estimates are negative for both outcomes. When the placebo is moved to 6 months before the true timing, all significant estimates are still negative. These tests offer strong evidence that the increase in violence is indeed driven by the introduction of the 3G network. Contour plots showing the results are presented in Figure 3.3, and detailed results of the analyses are presented in Appendix 3.D.

3.6.4 Additional Robustness Checks

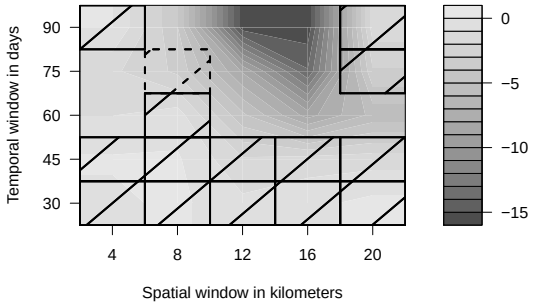
A proposition presented in Section 3.3 posits that the advantages of the 3G network regarding collective action primarily favour rebel groups, while not having meaningful impacts on the military operations of government forces. While the 3G network is a commercial technology that rebels are taking advantage of, government forces may already utilise communication technologies that are not commercially available, and they are also more likely to rely on face-to-face communication within their organisation. To test this proposition, I replicate the matched wake analyses using events that are coded as 'Friendly Action' in SIGACTs data. These entries are violent events initiated by the forces of Afghan government, the US or allies. The analyses yield mixed results that align with expectations. While only 8 out of 25 spatio-temporal unit sizes produce statistically significant estimates, 4 of these are negative, and the magnitudes of estimates are closer to zero, compared to the main analysis. When similar placebo tests are applied by shifting treatment events before 3 months of their original timing, the estimates are positive, suggesting that the positive estimates are



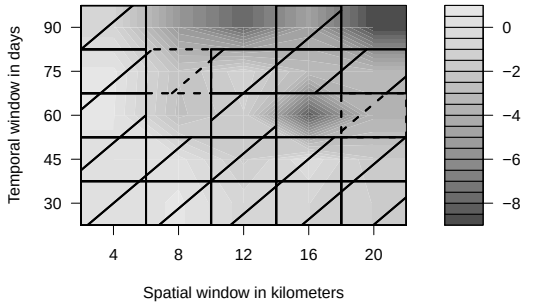
(a) DV: N. of Rebel Attacks
Placebo: 3 Months



(b) DV: N. of Rebel Attacks
Placebo: 6 Months



(c) DV: N. of IED Attacks
Placebo: 3 Months



(d) DV: N. of IED Attacks
Placebo: 6 Months

Contour plots showing the treatment effect estimates from the placebo regressions, with 2G as the control group and placebo 3G towers as treatment. Left-hand side plots show the effects of 3G 3 months before their installation, and right-hand side plots show the effects before 6 months of installation. The dependent variable is the number of violent events by insurgents for the above plots, and the number of IED attacks by insurgents for the below plots. In the clear areas, the estimate is significant at .05 level. Dotted areas are significant at 0.1, and in areas with solid lines, the estimate is insignificant. Note that all significant estimates are negative in all plots, providing evidence that the estimated effect of 3G is not driven by other factors. The plots are generated using `mwa` package in `R` (Schutte and Donnay, 2014).

Figure 3.3: Placebo tests for *H1* and *H2* (Matched wake analysis)

driven by other factors than the 3G network. When the placebo is moved to 6 months before treatment events, only six of the combinations produce interpretable results and all estimates turn negative. Overall, these tests support the argument that 3G network, as a commercial technology, does not have clear impacts on violence by government forces. Contour plots and detailed results for this analysis are presented in Appendix 3.E.

The findings are also robust to an additional set of different specifications and tests. An alternative operationalisation for multiple simultaneous attacks yields distinctly similar results to those of Table 3.3 and presented in Appendix 3.F. As noted in Section 3.6.2, spatial regressions with panel data covering the years 2009-2019 support the hypotheses. Regarding the matched wake analysis, the data sources on the covariates used in the matching provide the highest available resolution. Matching on covariates with lower resolution of 4 km and matching on district (*admin2*/Wuleswali) level covariates yield similar results. The telecommunication network is clustered in large cities in the early years of expansion, and Kabul City has the highest concentration. The findings are more robust, with estimates larger in magnitude when Kabul City is dropped from the sample. Finally, the results hold when the covariates used in matching are also included in the difference-in-differences regression.

3.6.5 Limitations

Although the findings provide strong evidence in support of the hypotheses, the study has several limitations. First, identifying a causal effect is challenging. There could be a complex set of factors which would prevent us from claiming the roll-out of 3G network infrastructure is orthogonal to conflict. Both the *push* and the *pull* factors during the roll-out may have been present. While consistent violence may have pushed expansion efforts away, companies appeared to be risk tolerant and bear costs. The government considered that expansion of the telecommunication infrastructure would increase economic activity and the tips from the local population about the insurgents. Therefore, consistent violence might also be a pull factor.

Second, it's important to note that the outcome of increased violence may not necessarily generalise across all conflicts and time periods. The central argument lies in the idea that the adoption of advanced communication technologies within an organisation improves information processing, decision-making, and operational efficiency. As such, while enhanced communication among insurgents aids in achieving organisational objectives, this translates into increased violence specifically within the context of high-intensity civil war. For example, during the recent Taliban takeover in Afghanistan in 2021, improved communications and effective propaganda might have facilitated the non-violent transfer of territory, as the Taliban acquired control over several military bases without using excessive force. Therefore, an increase in organisational effectiveness can produce different observable outcomes depending on the strategies and overarching goals of the organisation. In relation to this, observing the information flow within and between insurgents, militias, and active supporters is not possible, which leaves questions regarding micro-mechanisms remain unanswered.

Another limitation of the study comes from the network data. Although the Open Cell ID project provides a comprehensive and objective survey of cell phone network towers, it might not represent the universe of towers, but rather a subset of it. Although these limitations are mitigated by carefully designed analyses and robustness checks, the potential for future studies to benefit from higher-quality data remains evident.

3.7 Conclusion

This chapter contributes to the existing body of literature on the intersection of ICTs and conflict, and provides novel insights by focusing on the profound changes in modern communication technologies over the past decade. Specifically, it examines the potential impact of the third-generation mobile network on the levels of violence perpetrated by Afghan insurgents during an episode of high-intensity intrastate conflict. Using the Open Cell ID dataset for mobile networks and the SIGACTs dataset for insurgent attacks, it finds that the in-

troduction of 3G into the existing 2G network is associated with an increase in violence by Afghan insurgents, in various forms. However, it is useful to note that the increase in violence may not generalise to all civil wars, and this chapter argues that the impact of modern communication technologies hinges on their capacity to enhance organisational effectiveness. While increased organisational effectiveness can result in an improvement in the activities of the organisation, these activities may not exclusively entail the continuous engagement in violent attacks throughout a conflict. Sometimes insurgents strategically restrain violence and maintain low-intensity conflict. This dynamic can also partly explain the mixed findings in the literature.

The significant upsurge in cell phone usage within Afghanistan has brought about a transformation in the telecommunications sector, making it the largest employer and a rare success story in the country's economy even during the ongoing conflict (Shevory, 2016). The expansion of the telecommunication infrastructure garnered support and endorsement from both the Afghan government and US forces. This support was rooted in the belief that such expansion would not only foster economic progress but would also play a crucial role in counter-insurgency efforts by facilitating the collection of information and tips from locals. While these expectations were indeed plausible, a technology essentially serves as a tool, devoid of intrinsic benefits or harms. Its implications would depend on how and with what purpose it is being used. As new technologies are made available commercially, insurgents will adapt and try to use them to their advantage. Another recent and compelling example is the use of off-the-shelf drones by militants (Doctor and Walsh, 2021). Imposing restrictions on the commercial accessibility of such technologies solely due to their potential misuse by insurgents would be both unwise and unfeasible. Instead, the implementation of well-considered regulations and effective monitoring mechanisms can establish a viable foundation for a balanced and appropriate response strategy.

Appendix 3.A Detailed results for H2 (IED attacks)

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	30.00	4.00	0.62	0.03	0.12	339	157	0.90	7.20	0.77	0.14	59	70	0.75	21.40	0.51	0.29
2	30.00	8.00	2.00	0.00	0.29	339	157	0.93	4.90	0.82	0.23	64	91	0.83	10.80	0.60	0.44
3	30.00	12.00	2.15	0.00	0.41	339	157	0.95	3.30	0.84	0.27	61	75	0.87	7.20	0.66	0.52
4	45.00	4.00	1.15	0.00	0.36	339	157	0.90	7.70	0.78	0.15	58	77	0.84	13.50	0.54	0.31
5	45.00	8.00	1.83	0.02	0.42	339	157	0.95	3.60	0.84	0.26	63	62	0.87	9.90	0.65	0.46
6	45.00	12.00	3.59	0.00	0.48	339	157	0.91	6.70	0.86	0.30	57	82	0.95	3.70	0.73	0.54
7	45.00	16.00	4.50	0.00	0.41	339	157	0.94	4.90	0.87	0.32	57	65	0.94	4.90	0.75	0.55
8	45.00	20.00	4.74	0.00	0.43	339	157	0.94	4.90	0.87	0.32	55	55	0.93	4.80	0.75	0.57
9	60.00	4.00	0.95	0.05	0.39	339	157	0.94	3.90	0.81	0.16	59	77	0.87	8.50	0.56	0.33
10	60.00	8.00	4.14	0.00	0.51	339	157	0.96	3.20	0.86	0.27	63	72	0.85	11.20	0.68	0.48
11	60.00	12.00	3.05	0.01	0.49	339	157	0.94	4.80	0.88	0.31	56	50	0.93	5.80	0.75	0.55
12	60.00	16.00	4.65	0.00	0.38	339	157	0.96	3.60	0.88	0.32	53	47	0.92	5.70	0.77	0.57
13	60.00	20.00	4.89	0.02	0.29	339	157	0.96	3.60	0.89	0.34	45	44	0.73	18.00	0.77	0.59
14	75.00	4.00	1.57	0.01	0.33	337	146	0.94	4.20	0.82	0.21	55	72	0.86	10.00	0.59	0.36
15	75.00	8.00	2.88	0.03	0.53	337	146	0.94	3.30	0.87	0.30	47	54	0.92	5.10	0.70	0.52
16	75.00	12.00	6.49	0.00	0.61	337	146	0.95	3.40	0.89	0.32	48	47	0.94	5.30	0.76	0.58
17	75.00	16.00	8.43	0.00	0.69	337	146	0.98	2.60	0.89	0.33	48	42	0.92	6.70	0.78	0.60
18	75.00	20.00	5.96	0.00	0.60	337	146	0.97	2.90	0.89	0.34	44	43	0.93	4.90	0.78	0.62
19	90.00	12.00	5.30	0.00	0.71	336	146	0.98	2.20	0.89	0.40	48	55	0.96	2.90	0.77	0.62
20	90.00	16.00	6.90	0.00	0.66	336	146	0.97	2.10	0.90	0.40	42	46	0.87	10.70	0.79	0.62
21	90.00	20.00	11.55	0.00	0.53	336	146	0.96	4.10	0.90	0.42	57	37	0.93	6.30	0.79	0.68

Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and right-hand side, respectively. The *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

Table 3.4: Overview of the Matched Wake Analysis Results with IED Attacks as the Dependent Variable

Appendix 3.B Regression Results using GTD events

	DV: N. of Terrorist Attacks (*log*)			DV: N. of IED Attacks† (*log*)		
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Intercept		0.030***			0.023***	
		(0.004)			(0.003)	
2G Coverage$_{t-1}$	−0.017	0.036	0.007	−0.040	0.044	0.051*
	(0.034)	(0.034)	(0.034)	(0.025)	(0.026)	(0.026)
3G Coverage$_{t-1}$	0.338***	0.487***	0.202**	0.391***	0.501***	0.257***
	(0.061)	(0.079)	(0.072)	(0.044)	(0.059)	(0.055)
log Attacks$_{t-1}$		0.445***			0.414***	
		(0.006)			(0.006)	
ρ (Spatial lag of DV)		0.446***	0.588***		0.400***	0.446***
		(0.014)	(0.018)		(0.016)	(0.028)
θ_{2G} (Spatial lag of		−0.031	−0.061		−0.020	−0.064*
2G Coverage)		(0.041)	(0.041)		(0.031)	(0.031)
θ_{3G} (Spatial lag of		0.085	0.135		0.047	0.147*
3G Coverage)		(0.100)	(0.094)		(0.074)	(0.071)
λ (Spatial error parameter)		−0.310***	−0.494***		−0.289***	−0.367***
		0.023	(0.029)		(0.025)	(0.039)
District (Wuleswali) FE	✓		✓	✓		✓
Quarter-year FE	✓		✓	✓		✓
$t_{\beta_{3G}>\beta_{2G}}$	4.500	4.567	2.151	6.147	6.187	2.982
AIC	20496.26	22844.7	82428.34	9683.058	12835.76	71976.7
Log Likelihood	−9806.129	−11416.35	−40768.17	−4399.529	−6411.88	−35542.35
Num. of obs.	16716	16716	16716	16716	16716	16716
Num. of spatial units	398	398	398	398	398	398
Num. of time periods	42	42	42	42	42	42

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$. Standard errors are in parentheses.
Spatial units are secondary level administrative units (Wuleswali).
† Number of IED attacks is a subset of GTD events where the primary attack type is 'Bombing/Explosion' and the primary weapon type is 'Explosives.'

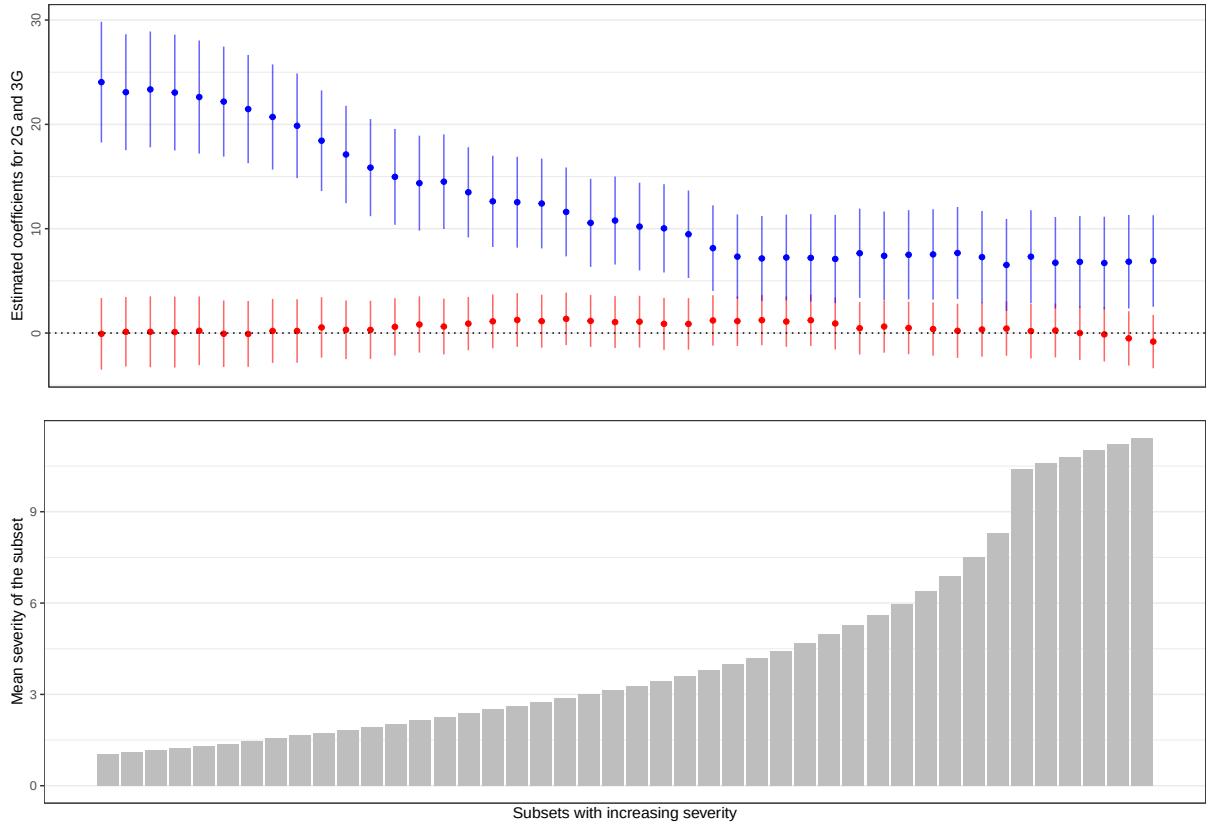
Table 3.5: Spatial and TWFE Regression Results with GTD data

Appendix 3.C Test of Potential Reporting Bias in GTD Between 2G and 3G Network Coverage

To further increase confidence in the results, I perform a diagnosis test based on a potential implication of the existence of reporting bias, following Weidmann (2016). The intuition behind this test is the proposition that the more severe events (i.e., with more casualties) are likely to be reported regardless of the coverage available, therefore, less susceptible to reporting bias. On the contrary, less severe events are more likely to be reported in areas with coverage. If GTD suffers from reporting bias, I expect that 3G coverage would have no (or smaller) effect on violence when I analyse events with high severity. To carry out the test, I ordered the events in 2018 by increasing severity.[13] Using a sliding window covering half of the events (N=886), starting from the least severe, I estimated a spatial general nesting model with variables of 2G and 3G network coverage and repeated this process moving the window 20 events upward each time. The results are plotted in Figure 3.4, with the coefficient estimates and confidence intervals of the 3G network variable shown in blue and the 2G network variable shown in red, while below histogram shows the mean severity of events in each subset corresponding to the estimates. In line with the results of Weidmann (2016), we see a downward trend in the 3G network coefficient as the mean severity increases in the subset, which is expected in a media-based event dataset. However, the decreasing trend gradually vanishes, and the estimates of the coefficient of 3G remain similar in almost half of the subsets with high severity, showing that the existing reporting bias in the data is not large enough to overturn the results. Indeed, with the subset of the most severe events, the coefficient value is approximately 7 and statistically significant. Considering the high values obtained with the subsets of less severe events, the results in the main analyses may represent an average effect. The original 'sliding window' test conducted in Weidmann (2016)

[13]The year here is chosen arbitrarily to rule out temporal dependencies in the subset.

estimates the effect of the 2G network alone and finds that the effect diminishes as the mean severity increases. However, the replication here increases confidence in the findings that the impact of the 3G network is profound and robust.



The coefficient estimates and 95% confidence intervals are in *red* for 2G network variable and are in *blue* for 3G network variable. Below panel shows the mean severity of events in each subset.

Figure 3.4: Testing potential reporting bias, adapted from Weidmann (2016)

Appendix 3.D Detailed Results of Placebo Tests

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	60.00	8.00	-3.04	0.04	0.43	339	165	0.98	1.60	0.86	0.30	36	50	1.00	0.00	0.67	0.33
2	75.00	12.00	-8.82	0.00	0.53	337	165	0.98	1.30	0.88	0.34	35	36	0.75	17.90	0.75	0.38
3	75.00	16.00	-10.61	0.01	0.52	337	165	0.99	0.70	0.89	0.35	38	26	0.91	7.50	0.77	0.38
4	90.00	8.00	-4.99	0.01	0.42	336	165	0.98	1.40	0.87	0.57	49	39	0.80	14.00	0.72	0.37
5	90.00	12.00	-15.12	0.00	0.62	336	165	0.99	1.00	0.89	0.64	37	37	0.89	8.30	0.76	0.39

Dependent variable: Number of attacks by insurgents. Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and right-hand side, respectively. *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

Table 3.6: Overview of the Placebo Test for *H1*: Installations of 3G Towers 3 Months Before the Original Date (Matched Wake Analysis)

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	30.00	20.00	-4.72	0.00	0.32	339	165	0.96	2.90	0.84	0.19	55	52	0.87	7.20	0.67	0.20
2	45.00	12.00	-5.60	0.00	0.53	339	165	0.97	2.80	0.86	0.20	45	51	0.92	6.10	0.72	0.21
3	45.00	16.00	-4.26	0.03	0.45	339	165	0.97	2.10	0.87	0.21	49	47	0.92	4.80	0.74	0.23
4	45.00	20.00	-7.89	0.00	0.49	339	165	0.99	1.30	0.87	0.21	58	41	0.91	7.90	0.74	0.25
5	60.00	8.00	-2.87	0.02	0.45	339	165	0.98	1.60	0.86	0.20	44	61	0.96	2.80	0.67	0.24
6	60.00	12.00	-6.20	0.00	0.45	339	165	0.98	1.40	0.88	0.23	38	49	0.91	7.10	0.74	0.27
7	60.00	16.00	-10.56	0.00	0.48	339	165	0.97	2.10	0.88	0.24	40	48	0.91	6.70	0.76	0.30
8	60.00	20.00	-6.67	0.03	0.22	339	165	0.97	2.10	0.89	0.25	44	31	0.91	5.70	0.77	0.34
9	75.00	8.00	-2.84	0.03	0.52	337	165	1.00	0.30	0.87	0.21	42	67	1.00	0.00	0.68	0.27
10	75.00	16.00	-5.63	0.03	0.33	337	165	0.99	0.70	0.89	0.26	46	47	1.00	0.00	0.77	0.32
11	90.00	8.00	-3.88	0.01	0.47	336	165	0.97	2.50	0.87	0.25	52	70	0.97	2.60	0.72	0.29
12	90.00	12.00	-7.92	0.00	0.61	336	165	0.98	2.30	0.89	0.28	41	44	0.95	3.80	0.76	0.32
13	90.00	16.00	-8.61	0.01	0.44	336	165	0.97	2.40	0.90	0.30	45	46	0.89	3.80	0.78	0.33
14	90.00	20.00	-10.20	0.01	0.37	336	165	0.97	2.40	0.90	0.30	48	33	0.90	5.40	0.78	0.37

Dependent variable: Number of attacks by insurgents. Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and right-hand side, respectively. *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

Table 3.7: Overview of the Placebo Test for *H1*: Installations of 3G Towers 6 Months Before the Original Date (Matched Wake Analysis)

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	60.00	4.00	-1.03	0.03	0.09	339	165	0.98	1.70	0.80	0.23	44	64	0.90	6.90	0.56	0.23
2	60.00	12.00	-4.75	0.02	0.31	339	165	0.97	2.10	0.88	0.34	23	27	0.89	6.50	0.74	0.36
3	60.00	16.00	-8.42	0.00	0.70	339	165	0.98	2.10	0.88	0.35	28	22	0.93	6.10	0.76	0.36
4	60.00	20.00	-5.69	0.05	0.27	339	165	0.98	1.40	0.89	0.38	28	25	0.93	5.60	0.77	0.37
5	75.00	4.00	-1.80	0.01	0.28	337	165	0.96	2.60	0.82	0.25	33	53	0.87	7.50	0.57	0.26
6	75.00	12.00	-8.13	0.00	0.52	337	165	0.98	1.40	0.88	0.34	29	24	0.97	2.90	0.75	0.38
7	75.00	16.00	-13.89	0.00	0.69	337	165	0.97	2.10	0.89	0.35	27	25	0.85	9.10	0.77	0.38
8	90.00	8.00	-3.94	0.02	0.30	336	165	0.97	2.10	0.87	0.57	26	16	0.61	30.00	0.72	0.37
9	90.00	12.00	-15.55	0.00	0.62	336	165	1.00	0.30	0.89	0.64	32	19	0.88	9.10	0.76	0.39
10	90.00	16.00	-15.69	0.00	0.63	336	165	1.00	0.30	0.90	0.66	27	17	0.93	3.80	0.78	0.40

Dependent variable: Number of IED attacks by insurgents. Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and right-hand side, respectively. *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

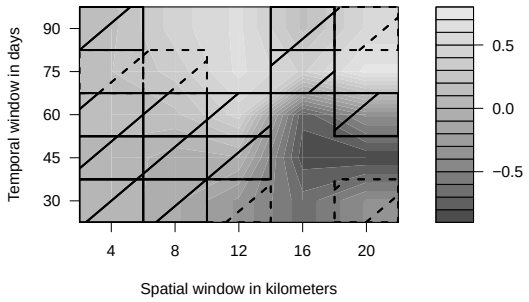
Table 3.8: Overview of the Placebo Test for *H2*: Installations of 3G Towers 3 Months Before the Original Date (Matched Wake Analysis)

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	60.00	8.00	-2.67	0.04	0.44	339	165	0.99	1.30	0.86	0.20	32	30	0.94	3.90	0.67	0.24
2	60.00	16.00	-8.46	0.00	0.33	339	165	0.98	1.70	0.88	0.24	26	33	0.79	15.00	0.76	0.30
3	90.00	8.00	-5.44	0.02	0.45	336	165	0.98	1.40	0.87	0.25	22	21	0.68	27.30	0.72	0.29
4	90.00	12.00	-7.97	0.00	0.70	336	165	0.99	0.30	0.89	0.28	22	20	0.91	6.90	0.76	0.32
5	90.00	20.00	-8.99	0.00	0.60	336	165	0.96	2.50	0.90	0.30	34	22	0.82	11.80	0.78	0.37

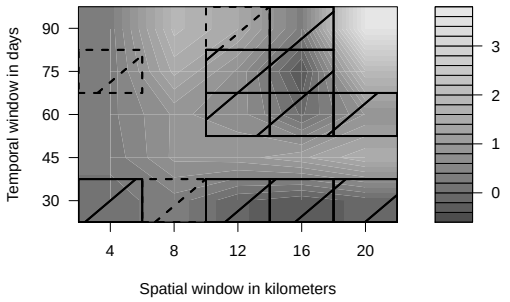
Dependent variable: Number of IED attacks by insurgents. Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and right-hand side, respectively. *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

Table 3.9: Overview of the Placebo Test for *H2*: Installations of 3G Towers 6 Months Before the Original Date (Matched Wake Analysis)

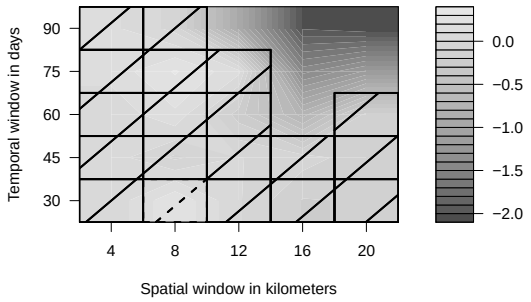
Appendix 3.E Effects of 3G on Attacks by Government Forces



(a) Original treatment timing



(b) Placebo: 3 Months



(c) Placebo: 6 Months

Contour plots showing the treatment effect estimates of the 3G network on the number of attacks by government forces, with 2G as the control group. The plot above shows the main estimates, followed by placebo treatments of 3 months and 6 months before the true treatment timing. In the clear areas, the estimate is significant at .05 level. Dotted areas are significant at 0.1, and in areas with solid lines, the estimate is insignificant. Note that the effect sizes are too small compared to main results, and the placebo test with three-month offset yields positive estimates. Overall, results here suggests that 3G might not have a clear effect on government attacks. The plots are generated using `mwa` package in `R` (Schutte and Donnay, 2014).

Figure 3.5: Effects of 3G Network on the Attacks by Government Forces (Matched Wake Analysis)

	Results					Placebo: 3 Months			Placebo: 6 Months		
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	Effect Size	p.value	adj.R^2	Effect Size	p.value	adj.R^2
1	30.00	16.00	-0.66	0.00	0.12						
2	45.00	4.00				0.26	0.02	0.03			
3	45.00	8.00				0.85	0.00	0.12			
4	45.00	12.00				0.92	0.00	0.14			
5	45.00	16.00	-0.85	0.00	0.09	1.16	0.00	0.24			
6	45.00	20.00	-0.88	0.00	0.07	1.56	0.00	0.26			
7	60.00	4.00				0.34	0.01	0.04			
8	60.00	8.00				0.83	0.01	0.09			
9	60.00	16.00	-0.77	0.05	0.10				-0.75	0.03	0.06
10	75.00	8.00				1.46	0.00	0.20			
11	75.00	12.00	0.63	0.03	0.03						
12	75.00	16.00							-1.44	0.00	0.57
13	75.00	20.00	0.74	0.03	0.18	1.97	0.00	0.18	-1.18	0.00	0.53
14	90.00	4.00				0.30	0.05	0.02			
15	90.00	8.00	0.45	0.03	0.05	1.87	0.00	0.25			
16	90.00	12.00	0.63	0.01	0.05				-0.93	0.00	0.64
17	90.00	16.00							-2.01	0.00	0.66
18	90.00	20.00				3.63	0.00	0.69	-2.07	0.00	0.42

Dependent variable: Number of attacks by government forces. Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Placebo tests for 3 months and 6 months before the true treatment timing are presented on the middle and the right-hand side, respectively. Only interpretable estimates are presented. Note that far fewer spatio-temporal combinations produce significant results compared to rebel attacks, and placebo tests show positive estimates can be spurious, indicating that the relationship is not clear.

Table 3.10: Overview of the Results with Government Attacks as the Dependent Variable (Matched Wake Analysis)

Appendix 3.F Regression results with the alternative definition of multiple coordinated attacks

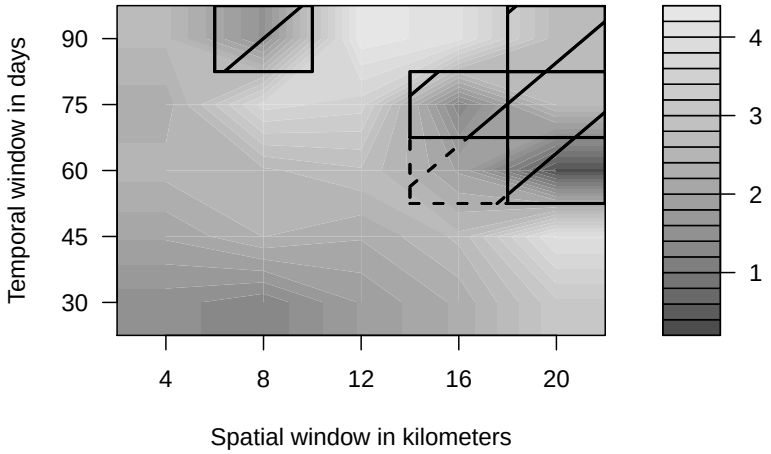
As an alternative measure of multiple simultaneous attacks, I code the number of individual events which are –potentially– a part of coordinated effort, by defining multiple simultaneous attacks as 'more than one violent event all of which happen on the same day and in the same province' (Afghanistan has 34 provinces). Although it is possible to coordinate simultaneous attacks across the country (or within a larger region than a single province), I limit the operationalisation to province level, since within larger areas it is difficult to distinguish whether these attacks are unrelated. However, it is very likely that militants operating within a single province know each other's activities and coordinate, both due to operational necessity and the likelihood of being from the same clan or tribe. These are more likely to be present in the context of Afghanistan, considering the nature of the Taliban, which is characterised by horizontal structures that reflect the segmented Pashtun tribal society (Ruttig, 2010). Replication analyses produce results that are distinctly similar to those of Table 3.3 and presented in Table 3.11 below.

	DV: N. of Coordinated Attacks (*log*)		
	Model 1	Model 2	Model 3
Intercept		$0.021(0.002)^{***}$	
2G Coverage$_{t-1}$	$-0.049(0.026)$	$-0.006(0.024)$	$-0.067(0.033)^{*}$
3G Coverage$_{t-1}$	$0.396(0.046)^{***}$	$0.440(0.055)^{***}$	$0.472(0.061)^{***}$
log Attacks$_{t-1}$		$0.095(0.002)^{***}$	
Spatial terms†		✓	✓
District (Wuleswali) FE	✓		✓
Quarter-year FE	✓		✓
$t_{\beta_{3G}>\beta_{2G}}$	7.395	6.466	6.971
AIC	11422.95	12430.68	73231.66
Log Likelihood	−5269.475	−6209.341	−36169.83

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$. Standard errors are in parentheses.
† Spatial terms include coefficients for the spatial lag of dependent variable (ρ), spatial lags of 2G and 3G coverage (θ_{2G}, θ_{3G}), and the spatial error parameter (λ).
A balanced panel dataset with 16716 observations (398 districts × 42 quarters) is used in all models.

Table 3.11: Regression results with the alternative definition of multiple coordinated attacks

Appendix 3.G Results including covariates in DD regression



Contour plots showing the treatment effect estimates from the difference-in-differences regression, with 2G as the control and 3G as the treatment group. The dependent variable is the number of violent events by the insurgents. In the clear areas, the estimate is significant at .05 level. Dotted areas are significant at 0.1, and in areas with solid lines, the estimate is insignificant. The plot is generated using `mwa` package in `R` (Schutte and Donnay, 2014).

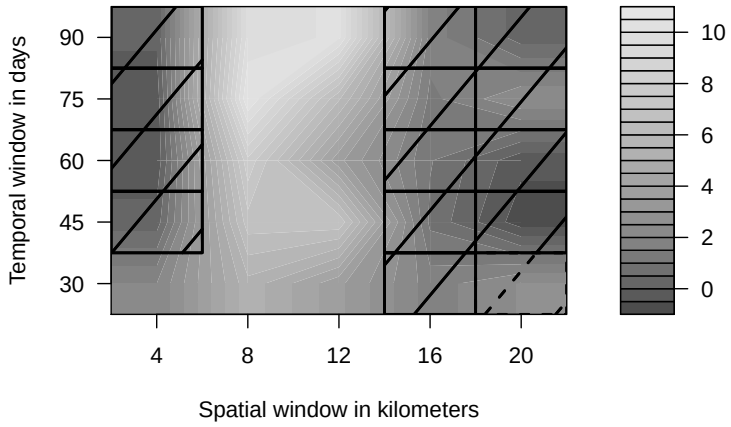
Figure 3.6: Results of matched wake analysis (with covariates included in DD regression)

	Results					Before matching						After matching					
	Time[days]	Space[km]	Effect Size	p.value	adj.R^2	control	treat.	L1	%CS	%SO	%MO	control	treat.	L1	%CS	%SO	%MO
1	30.00	4.00	1.49	0.00	0.45	0.06	0.00	0.28	0.09	0.88	156	-2.43	0.11	30.00	4.00	8.00	0.94
2	30.00	8.00	1.25	0.02	0.65	0.09	0.00	0.48	0.08	0.95	156	-4.74	0.07	30.00	8.00	3.70	0.95
3	30.00	12.00	1.82	0.00	0.62	0.07	0.00	0.28	0.37	0.93	156	-1.85	0.53	30.00	12.00	5.20	0.98
4	30.00	16.00	2.25	0.00	0.71	0.06	0.01	0.05	0.89	0.90	156	1.24	0.72	30.00	16.00	5.80	0.96
5	30.00	20.00	3.15	0.00	0.70	0.07	0.02	0.90	0.06	0.92	155	-5.44	0.23	30.00	20.00	5.70	0.96
6	45.00	4.00	2.03	0.00	0.46	0.07	0.00	-0.02	0.93	0.90	156	1.21	0.58	45.00	4.00	7.70	0.95
7	45.00	8.00	2.41	0.00	0.53	0.12	0.00	0.35	0.28	0.94	154	-3.03	0.33	45.00	8.00	4.70	0.96
8	45.00	12.00	2.22	0.00	0.58	0.15	0.00	0.15	0.69	0.94	156	-0.93	0.79	45.00	12.00	4.70	0.97
9	45.00	16.00	2.65	0.00	0.63	0.14	0.00	-0.26	0.52	0.94	154	3.10	0.42	45.00	16.00	4.40	0.97
10	45.00	20.00	4.04	0.00	0.73	0.11	0.01	-2.03	0.00	0.95	139	17.45	0.01	45.00	20.00	3.20	0.97
11	60.00	4.00	2.48	0.00	0.52	0.11	0.00	0.52	0.06	0.95	153	-5.24	0.04	60.00	4.00	3.40	0.97
12	60.00	8.00	2.56	0.00	0.50	0.15	0.00	0.64	0.10	0.96	151	-6.53	0.08	60.00	8.00	3.60	0.97
13	60.00	12.00	2.77	0.00	0.54	0.18	0.00	0.44	0.32	0.96	148	-4.25	0.31	60.00	12.00	2.80	0.98
14	75.00	4.00	2.29	0.00	0.51	0.09	0.00	0.40	0.22	0.95	131	-4.44	0.16	75.00	4.00	3.70	0.95
15	75.00	8.00	3.70	0.00	0.57	0.16	0.00	1.02	0.06	0.96	129	-10.87	0.04	75.00	8.00	3.00	0.94
16	75.00	12.00	3.50	0.00	0.57	0.19	0.00	0.65	0.28	0.97	131	-4.98	0.39	75.00	12.00	2.20	0.97
17	90.00	4.00	2.65	0.00	0.51	0.10	0.00	0.36	0.37	0.96	142	-1.50	0.69	90.00	4.00	2.30	0.98
18	90.00	12.00	4.33	0.00	0.51	0.16	0.00	0.34	0.63	0.97	139	1.74	0.80	90.00	12.00	2.10	0.98
19	90.00	16.00	4.06	0.02	0.59	0.14	0.03	-0.79	0.34	0.96	143	13.37	0.08	90.00	16.00	2.50	0.99

Results are presented on the left-hand side, with the sizes of spatio-temporal units used in estimation. Summary statistics of the sample before and after matching are presented on the middle and the right-hand side, respectively. *L1* distance metric and the common support summarise the similarity of the distribution of covariates between the treatment and control units. %CS: percentage of common support, %SO: percentage of same overlap, %MO: percentage of mixed overlap.

Table 3.12: Overview of the Matched Wake Analysis Results (with covariates included in DD regression)

Appendix 3.H Results excluding Kabul City



Contour plots showing the treatment effect estimates from the difference-in-differences regression, with 2G as the control and 3G as the treatment group. The dependent variable is the number of violent events by the insurgents. In the clear areas, the estimate is significant at .05 level. Dotted areas are significant at 0.1, and in areas with solid lines, the estimate is insignificant. The plot is generated using `mwa` package in `R` (Schutte and Donnay, 2014).

Figure 3.7: Results of matched wake analysis (excluding Kabul City)

Appendix 3.I Map of secondary level administrative units (Wuleswali)

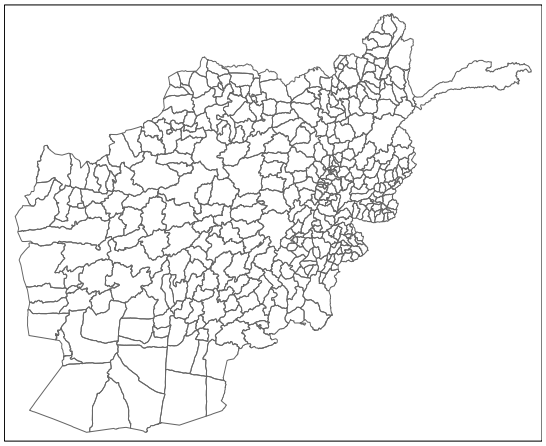


Figure 3.8: Map of 2nd Level Administrative Areas (Wuleswali)

Chapter 4

State Control Over Telecommunications, Surveillance, and Militant Mobilisation

Abstract

The ongoing debate on the effects of Information and Communication Technologies (ICT) on conflict focuses on the potential advantages that modern ICTs provide to the parties. While rebel groups utilise ICTs for propaganda and coordination, states capitalise on their control over network infrastructure for intelligence gathering and, in some cases, network shutdowns to disrupt rebel coordination. However, existing accounts often assume that states have total and constant control over the infrastructure, overlooking variations in ownership and control over telecommunication infrastructure between states and over time. This study aims to address this gap by investigating the link between state ownership of telecommunication companies and the emergence of rebel movements. I argue that state ownership and control over telecommunications facilitate surveillance efforts and elicit better information about opposition movements, enabling early detection and suppression of emerging rebel movements before they can pose a significant challenge to the government. Using newly released datasets on state ownership and control of telecommunications and militant mobilisation, I analyse this relationship with a sample of countries in Africa for the period between 2000-2012. The results indicate that state control over telecommunications is associated with a prolonged duration of mobilisation for armed groups, providing support for the argument.

4.1 Introduction

What are the implications of the age of digital surveillance for intrastate conflicts around the world? Do the states gain the upper hand against their non-state rivals by controlling the communication infrastructure? Previous research primarily focused on the revolutionary potential of modern communication technologies, testing the expectation that the proliferation of cell phones, the internet, and social media would trigger uprisings seeking more democratic governments or enhance armed mobilisation by reducing communication costs.[1] Studies on civil conflict produced mixed results (e.g. Bailard, 2015; Pierskalla and Hollenbach, 2013; Shapiro and Weidmann, 2015; Warren, 2014, for an overview, see Gohdes 2018), leading to a debate with pessimistic views suggesting that new communication technologies could increase repression, providing states with an asymmetric advantage (e.g. Morozov, 2011).

There has been little scholarly interest, however, in investigating the relationship between states' exploitation of modern communication technologies and civil conflict.[2] Empirical research on this subject has been hindered by data inaccessibility, and existing studies have primarily focused on investigating the link between armed violence and specific forms of digital repression, such as network shutdowns (Gohdes, 2020; Mustafa, 2023). Above all, when examining the interplay between states and armed groups, previous theoretical accounts have often assumed that states' control over telecommunication infrastructure is absolute and constant. However, this assumption is unlikely to hold true, as the extent of states' control over telecommunication infrastructure may vary both across different states and within the same state over time, influenced by various factors, particularly the relationship between

[1] Throughout the chapter I use modern communication technologies and modern ICTs interchangeably, defined as technologies (both hardware and software) enabling communications by electronic means such as mobile telephony, internet, and social media as well as the underlying infrastructure facilitating the exchange of electronic information. Similarly, telecommunication infrastructure is the facilities and systems for the transmission of information through various types of technologies.

[2] It should be noted that the effects of modern communication technologies have been studied extensively with regards to protests, contentious politics and polarisation (e.g. Diamond, 2010; Edmond, 2013; Manacorda and Tesei, 2020; Tufekci and Wilson, 2012; Weidmann and Rød, 2019), and theories in conflict studies are often borrowed from these areas of enquiry (Gohdes, 2018).

states and telecommunication companies.

This study aims to address this gap by focusing on the state's control over telecommunication infrastructure and its implications on civil conflict.[3] In particular, I argue that such control empowers governments to carry out surveillance effectively, allowing them to monitor dissent and obtain information about potential militant threats. This enhanced surveillance capability allows states to selectively target militants at an early stage, before an armed group can amass enough strength to challenge the state and escalate the conflict into a civil war. I consider ownership to be the most evident indicator of control, measured by the states' shares in telecommunication companies (Freyburg and Garbe, 2018).

Using recently released datasets on armed group mobilisation (Malone, 2022b) and ownership of telecommunication companies (Freyburg, Garbe and Wavre, 2023), I test these arguments for armed groups in Africa for the period between 2000-2012.[4] Africa represents a compelling case for examining the impact of modern communication technologies, as the proliferation of cell phones and mobile internet has been rapid across the continent, while fixed lines have remained severely limited. According to the International Telecommunications Union (ITU), 198 million of the 221 million total telephone subscribers in Africa were mobile cellular subscribers in 2006, which was the highest ratio of mobile phone users to total telephone subscribers in the world (ITU, 2008). This gap continues to widen and by 2021 there are 83 mobile subscriptions per 100 people in Africa, compared to 0.6 fixed line subscriptions (ITU, no date).

I expect that an increase in the state's share of telecommunication companies would lead to a prolonged duration of mobilisation, defined as the period between the formation of the armed group and the escalation into civil conflict. The results show nearly an 87% decrease

[3]I use civil conflict and intrastate conflict interchangeably, and refer to Uppsala Conflict Data Project (UCDP) to define *civil conflict*: A contested incompatibility that concerns government and/or territory where the use of armed force between a government and a non-governmental party results in at least 25 battle-related deaths in one calendar year (Themnér and Wallensteen, 2014).

[4]Following Malone (2022b), I define an armed group as "an independent organisation of non-state actors that justifies the use of violence in the pursuit of political control." This broad definition includes rebel groups, terrorist groups, anti-government militias and violent political parties, while excluding criminal actors, individuals, pro-government militias and factions of existing groups (Malone, 2022b, p.3).

in the hazard rate when a state holds full ownership of ISP companies, compared to states with no share, and these results remain robust to several alternative specifications and tests. Overall, the study advances our understanding of the relationship between ICTs and armed conflict, while also contributing valuable insights to the existing literature on state capacity, surveillance, and repression. In the remainder of the chapter, I first present an overview of the literature and the research gap motivating the study. I then provide a detailed elaboration of the argument, followed by the presentation of the data and the analysis. I conclude with a discussion of implications and avenues for future research.

4.2 Overview of the literature and motivation

The proliferation of modern communication technologies has sparked considerable interest among researchers studying conflict and protest, leading to a profound debate surrounding the potential effects of these technologies on contentious politics. Theoretical discussions have proposed various implications, offering insights into their potential impact. For instance, if these technologies can effectively address collective action problems, we might observe an increase in protests and the onset of civil conflicts. Furthermore, the dissemination of information on government activities through these mediums could amplify dissent among citizens, further fuelling protests. Similarly, if the enhanced communication capabilities facilitates propaganda efforts, insurgent groups might be able to recruit more militants, increasing intrastate conflicts and their intensity. On the other hand, if these technologies provided new means of repression for the states, we should expect a decrease in both protests and conflict. Modern ICTs have been argued to facilitate new and effective means of surveillance and consequently selective targeting of insurgents. It is also argued that governments can use their control on ICT infrastructure to undermine rebel collective action by applying network shutdowns.

The empirical picture is more complicated than suggested by the theory. There are dif-

ferent types of technologies, evolving over time and often intertwined with each other (e.g., the internet, mobile phones, social media). For investigating the impact on collective action, off-the-shelf technologies with widespread presence hold significant relevance. These technologies are accessible to the general public, fostering connections among ordinary citizens, and some even create a public space for communication. However, their presence is not random, which poses challenges in identifying credible effects or lack thereof. Arguments in favour of a positive effect on conflict have been tested using event data and network coverage/access and the results are mixed (e.g. Bailard, 2015; Pierskalla and Hollenbach, 2013; Shapiro and Weidmann, 2015).

Studying governments' exploitation of communication technologies presents less promising prospects for scholars. The scarcity of information hinders systematic data collection in a cross-country setting. States tend to be reluctant to disclose any information regarding their surveillance capabilities and activities. Additionally, domestic legal frameworks may not be representative in terms of the actual practices, as numerous incidents have exposed that existing laws meant to restrict governments are sometimes disregarded, even in democratic countries (Privacy International, 2019). Furthermore, the diverse nature of these technologies offers a wide range of surveillance capabilities. States can intercept communications through companies providing network services or opt for third-party hardware and software for interception without the involvement of network companies. Other methods include the use of facial recognition technology and closed-circuit television (CCTV) systems.

The limited availability of observational data has constrained empirical research on this subject, resulting in only a few studies. Gohdes (2020) and Mustafa (2023) have examined the impact of network shutdowns at the subnational level in Syria and Pakistan, respectively. Gohdes (2020) reveals that areas with limited internet access experience untargeted repression from the state, while Mustafa (2023) demonstrates that the number of terrorist attacks decreases during cell phone network shutdowns, but increases after the shutdowns end. Existing studies that examine the effect of communication technologies on conflict attribute

a decrease in conflict to an increase in tips from the local population about the insurgents and the improved opportunities for signal intelligence (Shapiro and Weidmann, 2015). Conversely, other studies find evidence supporting the collective action hypothesis, indicating an increase in conflict (Pierskalla and Hollenbach, 2013).

Theoretical perspectives often implicitly assume that states have absolute and constant control over telecommunication infrastructure, including the ability to employ complete network shutdowns and interception. However, this assumption may not reflect the complex reality. States possess varying bureaucratic or administrative capacities to enforce their policies, with 'capacity' being defined and measured in different ways (Hendrix, 2010). Mann (1984, p. 189, 2008) defines state *infrastructural* power as 'the capacity of the state to actually penetrate civil society, and to implement logistically political decisions throughout the realm.' Similarly, Yashar (2005, p. 6) maintains that state's *reach* across its territory is 'the state's actual penetration throughout the country and its capacity to govern society,' which can be uneven even within a single country.

States with high levels of bureaucratic or administrative capacity are argued to possess the ability to address potential challengers by redistributing resources, and those with high levels of military capacity can repress dissidents effectively (Hendrix, 2010). Dissidents are expected to take into account the capacity of the state to repress or accommodate before deciding to rebel, and studies indicate that both forms of capacity are associated with a lower likelihood of intrastate armed conflict (Hendrix and Young, 2014). Besides the ability to accommodate, higher bureaucratic or administrative capacity enables states to extract more information from local populations, through means such as registering citizens or monitoring them (Soifer, 2008). Possessing higher 'infrastructural' power and control allow states to acquire more information, potentially reducing the likelihood of armed conflict as they gain the capability to identify, monitor, and target dissidents and rebels (Fearon and Laitin, 2003; Hendrix and Young, 2014; Soifer and vom Hau, 2008).

While the expansion of telecommunication network requires outreach across the country's

territory, access and control over telecommunications tend to be more centralised. This implies an advantage and may incentivise states to access and monitor telecommunication networks. Such access would help states obtain information about the population, including dissenters, which would otherwise require more financial and human resources invested in bureaucratic power and outreach.

The state's ability to exercise control over telecommunication infrastructure is likely to be shaped by the relationship between the government and telecommunication companies. Ownership structures of these companies can offer insights into the extent of state access and control, especially when the companies are owned by the state itself or by elites closely aligned with the government (Freyburg and Garbe, 2018). Additionally, companies that are not owned or controlled by the state may still comply with government requests for access or information in specific circumstances. Moreover, states may possess the ability to intercept and access telecommunication networks using advanced surveillance tools, without the knowledge of the companies providing the services. Such characteristics can vary between countries and over time. Changes in control may arise due to the nationalisation or privatisation of telecommunication companies, while access to advanced surveillance products is subject to economic power and diplomatic relations, as companies offering such products often encounter export restrictions.

Repressive policies targeting violent or non-violent dissent encompass a variety of practices carried out by government authorities. Among these, exploiting control over telecommunication infrastructure to employ repressive measures in the digital sphere is just one type, often complemented by several others. The repertoire of digital repression also includes various methods, such as surveillance, digital censorship, or network shutdowns.[5] The selection and intensity of these measures are likely to be tailored considering the nature of the threat.

[5]Network shutdowns on internet and mobile services are increasingly employed by governments worldwide, with varying justifications. The extent of these practices also spans a continuum, ranging from complete blackouts to slowing down connections or selectively blocking specific platforms. The time frames for these shutdowns can range from a few hours to several months or even years (Feldstein, 2022). *Access now*, an organisation documenting internet shutdowns, reports different types of triggers for network shutdowns, such as protests, elections, armed conflicts, coups, and school exams. (Hernández et al., 2022).

For instance, even if the government conducts surveillance and identifies a network of individuals, it may lack the capability to selectively target militants if an armed group has already escalated the conflict and gained enough power to challenge the state. The security apparatus of the state might be unable to access these individuals if the government lacks territorial control in their location or if the government can only access those areas through large-scale military operations. In such cases, governments may resort to network shutdowns to undermine rebel collective action and employ indiscriminate violence to re-establish control, especially during military offensives. Digital censorship practices are also evolving as a form of network interruption. Blocking websites or social media applications and removing content from the web are used as selective means to restrict public access to information.[6] In the context of civil conflict, digital censorship practices can be implemented to limit or prevent online propaganda activities targeting governments. While these methods represent a comprehensive policy with complementary measures, this study exclusively focuses on the relationship between surveillance and early-stage armed mobilisation, as theorised in the following section.

4.3 Surveillance against mobilisation

Throughout history, states have engaged in the practice of collecting information about their citizens and their preferences as a proactive measure to ensure regime security. By constantly staying updated on the status of dissent among the population, states and regimes seek to prevent potential uprisings from reaching a critical level where the state's ability to enforce public order might be compromised. Especially in regimes where alternative means of obtaining information about the preferences of citizens, such as free media, elections, or freedom of speech, do not exist, surveillance can influence regime behaviour and shape strategies of

[6]While some of these practices are implemented permanently without any clear time frame for easing restrictions, their successful application depends on the governments' capacity to manage the communication infrastructure, and methods to circumvent these measures are available in some countries (Feldstein, 2022).

repression and co-optation by providing information about dissent and potential uprisings (Xu, 2021). Furthermore, surveillance is a tool for domestic security, safety, and crime prevention, which is relevant for states of all regime types. Security and intelligence agencies of countries allocate some of their resources to address perceived threats within their own populations.

In the context of state surveillance, armed uprisings and organised violence stand in between two objectives. They emerge from broader dissident movements and draw their strength from the support of a part of the population. By conducting mass surveillance of the population, governments can gain insights into the level of popular support enjoyed by these armed non-state actors. Organised violence also entails a 'criminal' aspect that poses a threat to public order. These groups exhibit an organisational structure involving decision makers, logistics and combatants, who collectively execute violent actions against government or civilian targets. Information regarding the general dissent among citizens may not suffice to identify the network of individuals orchestrating the armed organisation, and a more focused targeted surveillance may be needed which enable governments to selectively target those individuals (Dimitrov and Sassoon, 2014). While surveillance is just one form of repression among many, it may be more convenient for states as it can enable selective targeting and reduce the likelihood of backlash compared to other indiscriminate methods (Daxecker, 2017; Young, 2013).

Surveillance poses practical challenges for both states and armed groups. For dissidents organising a rebellion, effective communication and coordination are essential, despite the risk of exposing themselves and their true preferences to the state. On the other hand, employing surveillance is a costly endeavour, especially on a mass scale. However, these dynamics are subject to change as modern telecommunication technologies are becoming the prominent means of communication with widespread use. The decrease in communication costs may help dissidents with coordination and collective action,[7] while also making it easier

[7]Modern ICTs are argued to ease collective action and free-riding problems by decreasing the communication costs and establishing continuous lines of communication within groups (Pierskalla and Hollenbach,

for states to employ mass surveillance in the digital realm. It is essential to acknowledge that digital surveillance complements other methods within overall surveillance efforts rather than replacing them. Nevertheless, it proves to be comparatively easier than physical surveillance, as it allows information to be captured at various 'nodes,' often irrespective of geographical distance.

The surveillance of communications requires some sort of control over or access to telecommunication infrastructure. For states, this control can be in the form of ownership of telecommunication companies and/or having regulatory authority over the telecommunication sector in their countries. This implies that states have an asymmetrical advantage over dissidents or rebel groups. Not only can they own shares in companies that operate telecommunication networks, but they also possess the authority to regulate the sector and decide which private companies can operate within their territory. For instance, states often require private companies to provide access to their networks as a prerequisite to enter the domestic market (Roberts et al., 2021). Such control over telecommunications can facilitate continuous surveillance of populations, allowing government agents to gather information about opposition activities and status.

While telecommunication companies can provide security agencies of the state with direct access to their databases and call records for monitoring purposes, they can also allow indirect access by complying with information requests from government authorities. Both states and telecommunication companies can utilise third-party hardware or software for intercepting or intruding communications. Indeed, there exists a global business market for surveillance products, aiming at states and telecommunication companies as customers. Although such companies often lack transparency regarding their sales and transactions, many of them participate in trade fairs related to military, security, or surveillance themes to promote their

2013). This would lower the threshold for the ability to coordinate and make it easier to organise an armed group compared to the pre-ICT era (Walter, 2017). These technologies also facilitate the rapid and widespread dissemination of information, allowing it to reach every segment of society and increasing citizens' awareness of government activities, increasing scrutiny. This may increase dissent among citizens, which may lead to more protests or violence as a result (Bailard, 2015).

products. A report compiled by Privacy International identifies 528 companies operating in the surveillance industry through attendance to trade fairs and open-source information (Privacy International, 2016).[8] Another report suggests that sales of surveillance products between non-allied countries (e.g. a company with headquarters in Europe selling products to Russia or China) are prevalent (DeSombre, Gjesvik and Willers, 2021). Such commercial products include, but are not limited to, systems for internet, phone, and location monitoring, audio and video surveillance and analysis software (Privacy International, 2016, p. 20).

Control over telecommunication infrastructure and companies is prone to be exploited in several ways, and practical applications are evolving over time. An illustrative example of surveillance methods employed by government security agencies can be found in a report by Privacy International, which focuses on counter-terrorism efforts in Kenya (Privacy International, 2017). The extent of power granted to government authorities under legal frameworks can vary between countries, but they often leave room for circumvention. In the Kenyan case, the law grants extensive power to security institutions, with ambiguous framing open to varying interpretations. For instance, the Prevention of Terrorism Act codified in 2012 grants the Kenyan Police the right to enter the premises of telecommunication companies to install monitoring devices, without any definition of a permitted device (Privacy International, 2017, p. 12). The National Intelligence Service of Kenya also circumvented certain restrictive regulations by first conducting surveillance on targets without judicial permission or oversight and then transferring the case to law enforcement agencies to obtain the required judicial approval (Privacy International, 2017, p. 16). Furthermore, telecommunication companies were hesitant to reject unlawful requests of information by government authorities, with the fear of reprisal such as revoking of companies' licences. In some countries, telecommunication companies are legally required to install monitoring devices to their network, or to host liaison officers from security agencies in their premises, permitting access to their data.

[8]This number does not include companies selling relatively unsophisticated technologies, and the authors of the report acknowledge that it under-represents companies from Russia and China (Privacy International, 2016, pp. 12-14).

Such information channels can provide government agencies with call data records (which includes information on the initiator of the call, receiver, location of the base transmitter station where the call is made, type and the duration of the call), SIM card registration and mobile money databases. With additional capabilities, this can include live tracking of individuals' locations and listening voice calls. Security agencies can then use these information to analyse the activities of militants, predict their actions, and selectively target or arrest them.

Continuous surveillance of populations enables governments to detect potential or emerging uprisings and suppress rebel movements before they can mount a significant challenge to the state. Insurgent groups typically emerge out of political movements, but differ from them as they build an organisation including logistics, finances, combatant units, and command and control structure. Especially financial and logistical structures play crucial roles in this transformation and without them 'organised armed rebellion reduces to violent protest' (Parkinson, 2013, p. 418). Monitoring of communications can help the government identify a network of individuals involved in building armed organisations and target them in the early stages of their formation. Mass and targeted surveillance here are not substitutes but rather complementary. Mass surveillance continuously identifies specific targets to focus on for further in-depth surveillance. However, mass surveillance is typically more labour intensive and more costly (GMacAskill et al., 2013). Monitoring high numbers of people requires either a large number of workforce or expensive artificial intelligence (AI) solutions.

Government-owned companies are more likely to cooperate and provide access to state security and intelligence organisations when requested. Private companies, on the other hand, may face a variety of incentives and restrictions. While private companies have an interest in protecting the privacy of their customers, they may also have to adhere to specific government requirements to obtain a licence and operate within a country. This can include agreements to provide data to governments for security, terrorism, or crime prevention purposes, within the bounds of relevant regulations. Private companies may also choose to acquiesce to unlawful

demands from governments to avoid potential repercussions (Privacy International, 2017, p. 17; Mare, 2020). Domestic companies may be likely to have closer ties to the government elite and may be more inclined to comply with government requests. In contrast, international telecommunication companies may have fewer incentives to comply with unlawful demands, particularly if such actions could tarnish their global reputation or lead to legal consequences in their home countries.

An illustrative example is the events that led to the sale of Telenor Myanmar, a subsidy of the Norway-based telecommunication company Telenor. Following the military takeover in Myanmar on 1 February 2021, telecommunication companies operating in the country faced pressure from the Myanmar military to comply with repressive measures, including network shutdowns and the activation of intercept equipment to monitor communications. While Telenor could not prevent the network shutdowns, it resisted the requests to activate the intercept equipment (Telenor Group, 2021a;d). However, maintaining such a stance proved to be challenging and unsustainable, and the company eventually had to consider the possibility of leaving the country (Telenor Group, 2021c):

> 'It has become clear to us that our continued presence would require Telenor Myanmar to activate intercept equipment (for the use of Myanmar authorities) which is subject to Norwegian and international sanctions. Activation of such equipment is therefore unacceptable for Telenor Group. Furthermore, as a legal and regulatory framework that safeguards our customers and adheres to fundamental human rights and international laws is not in place in Myanmar now, operating such equipment in this situation would constitute a breach of our values and standards as a company. Ultimately, this conflict between local and international law and human rights principles makes continued presence in Myanmar impossible for Telenor Group'.
>
> 'Having worked actively to avoid activation of intercept equipment, Telenor Myanmar Ltd. has until now not activated this equipment and will not do so voluntarily. Due to well-funded concern for the safety of our employees, we will unfortunately not be able to comment further on the government directive to implement intercept equipment beyond today's update' (Telenor Group, 2021b).

This anecdote shows that even during an episode of severe repression, foreign-owned telecommunication companies may have more leeway compared to state-owned or national companies. However, stuck between local law and employee safety on the one hand, and the international law and human rights, as well as the scrutiny by the international community on the other, Telenor sold its subsidy in Myanmar to the Lebanon-based M1 Group. The approval of this sale was conditional on M1 Group ensuring the majority of the company is locally-owned, and immediately after the sale Shwe Byain Phyu, a company linked to the Myanmar military, acquired 80% of the shares. This can be considered as an indicator of governments' intention to secure control over telecommunications by securing government ownership. Although Telenor ultimately could not resist and stay in Myanmar, the change in government control was effectively achieved through the change in ownership. As part of the sale, the call traffic and personal data of 18 million users were transferred, leading to concerns raised by non-governmental organisations in Myanmar about potential human rights abuses by the military authorities (Telenor Group, 2021e). Telenor did not prevent the transfer of the data over safety concerns of its employees (Telenor Group, 2022).

Countries often have legal frameworks that outline restrictions on government access to private communication data and surveillance. These frameworks typically require a judicial order to monitor individuals' communications, and specify the types of crimes for which such powers can be invoked. However, in practice, these legal boundaries can be bypassed by state security agents. For example, even in the presence of judicial independence, law enforcement or intelligence agents may manipulate the system by adding the phone numbers of political opponents to a list of suspects of ordinary crimes. By obfuscating them among criminals, they can obtain the approval of a judge, allowing them to monitor these individuals' communications (Right2Know, 2016, p. 14). These regulations are also vulnerable to loopholes with the ever-changing nature of communication technologies (e.g., Groenewald, 2017; Roberts et al., 2021). While in some countries regulations may not exist at all, in many countries existing laws are suspected to be breached.

The argument presented in this study is based on the assumption that states will take advantage of opportunities for surveillance. However, the willingness of government elites to exploit their access and power over these companies, along with the absence of effective oversight, are crucial factors that influence the likelihood of extralegal surveillance practices. The quality of judicial processes and the rule of law can provide insights into the potential restraints that a government may have in exploiting its control over telecommunications companies. Although there is no conclusive evidence as state surveillance activities rarely get revealed and publicised, it is worth noting that even democratic countries with robust oversight mechanisms have been involved in controversial mass surveillance activities. For example, the United States of America and the United Kingdom used their technological capacities to monitor all digital information flow in and out of their countries, although they claim to target international threats rather than domestic threats (Privacy International, 2019).

While I propose that state ownership of telecommunications facilitates surveillance and helps governments degrade resistance movements before they evolve into armed conflict, this link may be conditional on network penetration, as gathering information through the monitoring of telecommunications would be limited to its outreach. In other words, states can only conduct communication surveillance on targets who have access to these networks. The expansion of cell phone networks and internet access within countries typically starts in urban areas, gradually spreading across the country and increasing the area of coverage. The proportion of the population having access is often taken into account when measuring the effect of ICT on various outcomes, such as economic growth (e.g. Aker and Mbiti, 2010; Roller and Waverman, 2001; Vu, 2011), as this reflects the presence or dose of the 'treatment.' Increasing network penetration, i.e., an increasing proportion of people having connection to mobile network or internet, would naturally increase the amount of information gathered by the digital surveillance activities. Therefore, the outreach of state surveillance through telecommunication channels would vary over time and space during the roll-out of commu-

nication network infrastructure, depending on the portion of the population with access to telecommunications.

H1: As the state's share of telecommunication network companies increases, escalating into a civil conflict would take longer time for an armed group.

H1a: As the state's share of telecommunication network companies increases and *network penetration increases, escalating into a civil conflict would take longer time for an armed group.*

4.4 Data

4.4.1 Dependent variable

Emerging rebel movements, if mobilised successfully, follow a common path toward escalation. The formation of a group is followed by the initiation of the armed struggle, marked by the first attack of the group. If the rebel group can maintain momentum and continue committing attacks, this would evolve into a civil conflict. I adopt the definition of the UCDP and use a threshold of 25 battle-related deaths to identify armed struggles that escalate into civil conflict. Figure 4.1 illustrates this path, where some armed groups achieve to proceed the next stages and escalate above the threshold level, while others fail to do so. For example, in Nigeria, Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād, known as Boko Haram, was founded in 2002, conducted its first attack in 2007 and the violence escalated into a civil conflict in 2009 with a series of clashes with the police forces. Note that while the formation and the first attack must be separate stages, information on the timing of these would be limited, as many groups claim their existence with their first attacks due to the clandestine nature of the group formation. Similarly, if the first attack results in battle-related deaths above the threshold, the dates for first attack and civil conflict onset would overlap.

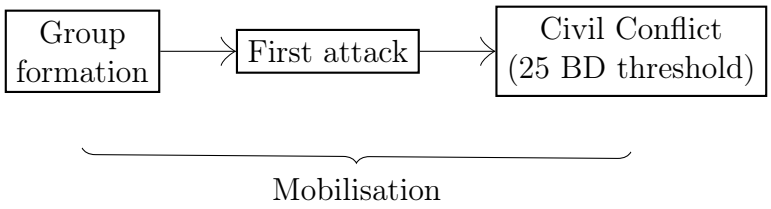


Figure 4.1: Armed group mobilisation

For information on the emergence of armed groups and their (non-)escalation into armed conflict, I use the Armed Group Dataset (AGD) (Malone, 2022b) which provides an overview of armed groups that operated around the world between 1970 and 2012, including information on the year of group formation, first attack, and conflict onset, as well as organisation level attributes.[9] The distinctive feature of AGD is the effort to compile all armed groups regardless of their success to escalate into civil conflict and to end up in civil conflict datasets.

I define *mobilisation duration* as the time between the formation of an armed group and civil conflict onset, during which they engage in political violence. If an armed group stops using political violence before crossing the threshold of civil conflict, due to reasons such as disarming, disappearing, being defeated, merging, or splintering, this is considered an unsuccessful mobilisation attempt.

4.4.2 Independent variable

I consider ownership of telecommunication companies as an indicator of control over telecommunications. The state's access to information and control over infrastructure likely depend on the government's relationship with the owners of these companies. Foreign companies may have different incentives and restraints compared to state-owned or domestically owned companies when it comes to complying with lawful or unlawful requests from governments.

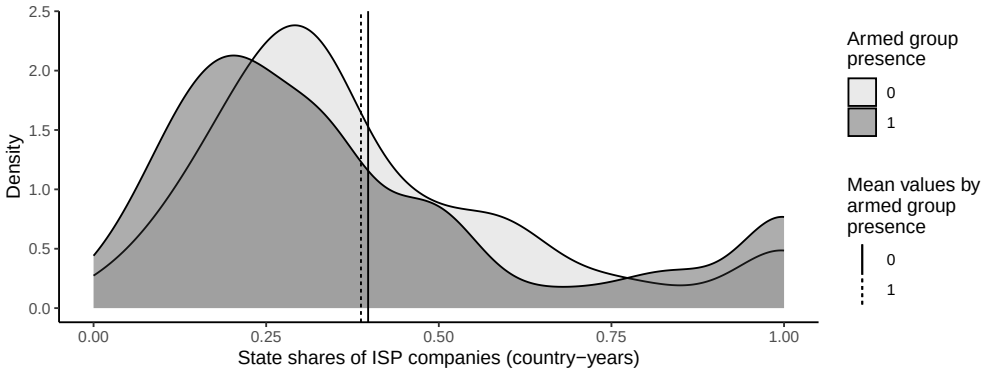
For information on state ownership of telecommunication companies, I use the Telecommunications Ownership and Control (TOSCO) dataset (Freyburg, Garbe and Wavre, 2023),

[9]Available at: https://armedgroupdataset.org/. AGD is built on the population of armed groups introduced in the Terrorist Organisation (TORG) Crosswalk (Asal, Cousins and Gleditsch, 2015), which records all groups with at least one attack in the Global Terrorism Database. AGD uses qualitative resources to identify groups within that population that fit its definition of an armed group (Malone, 2022b).

which covers all internet service provider (ISP) companies operating in 49 countries in Africa that are members of the Global System for Mobile Communication (GSM) Association during the period between 2000 and 2019. The dataset focuses on 'telecommunication companies that have a physical presence in the area which they operate, hold official state licences to operate cables, and own the communication infrastructure they use,' resulting in a total of 196 companies. Throughout Africa, mobile phones are predominantly used to access the internet, and the roll-out of mobile network infrastructure preceded the fixed lines in many areas (Pierskalla and Hollenbach, 2013). The dataset includes companies providing service starting from 2G standards and running their own infrastructure, while excluding companies offering only 3G, 4G, and Mobile Virtual Network services by renting the necessary infrastructure from the companies already included in the TOSCO dataset (Freyburg, Garbe and Wavre, 2023, p.9). Therefore, the data set practically covers most of the mobile phone and internet communications on the continent.

Following Freyburg, Garbe and Wavre (2023)'s approach, I use aggregated shareholder information of telecommunication companies by country, retrieved by dividing the total amount of shares of the state by the number of companies in the country. This leaves me with values ranging from 0 to 1. Figure 4.2 shows the distribution of values with and without any armed group presence, indicating that there is no clear tendency for countries subject to militant mobilisation.[10] Mean values for state shares with or without the presence of armed groups are similar (0.39 and 0.40, respectively), and a Welch t-test confirms that they are not statistically different (p-value = 0.69).

[10]One concern about the countries where all telecommunication companies are state-owned is this situation may be driven by the lack of private investment due to reasons such as instability or state weakness, thus these states end up having to provide telecommunication services themselves. However, mobilisation of armed groups should be easier in such unstable countries experiencing a lack of state authority, which implies the reverse of the proposed relationship, biasing the results against the hypothesised direction, if applicable.



Country-years with at least one armed group presence are in dark shaded color.

Figure 4.2: Density plot of state shares of ISP companies by country-years (2000-2019)

4.4.3 Confounders

To ensure the reliability of any conclusions regarding the association between armed mobilisation and telecommunication ownership by states, several confounding factors must be considered. A significant factor is the outreach of the telecommunication network, which may vary over time and across countries with different levels of development. To address this, I incorporate data on mobile cellular subscriptions per 100 people from the International Telecommunications Union (ITU). Additionally, I account for the number of Internet Service Provider (ISP) companies in each country. While the main independent variable is the average state shares in these companies, countries may have different market structures, with some having monopolies over telecommunications, while others exhibiting more competitive environments with involvement from private or international companies. These structures can influence incentives and relationships with the state.

The leeway of governments to exploit their control over the telecommunication infrastructure and conduct indiscriminate surveillance may depend on the restrictions exerted over them by judicial institutions. Although these restrictions can be bypassed in many cases, the extent of surveillance may be greater in a context where no judicial control is exercised on the executive. On the contrary, strong judicial institutions can be a deterrent for governments intending to commit unlawful surveillance practices. To capture compliance with the

judiciary, I use 'Judicial constraints on the executive index' (v2x_jucon) from the Varieties of Democracy (V-Dem) data, which includes scores on compliance with judiciary, compliance with high court, high court independence, lower court independence and respect of the executive to the constitution (Coppedge et al., 2022).

Surveillance on its own merely provides governments with *information* about the activities and whereabouts of individuals within the armed organisation. Its impact on mobilisation is contingent upon the government's ability to take action based on that information, selectively arresting or targeting militants. If governments lack the capacity to effectively conduct counter-insurgent operations, whether through law enforcement or military means, surveillance may have limited effectiveness. To account for the military and law enforcement capabilities of states, I utilise data on military expenditures from the National Material Capabilities Dataset of the Correlates of War project (Singer, 1988).

Additionally, several prominent factors that might change the overall propensity of states to experience armed rebellion are also controlled for. Higher state capacity is associated with a lower propensity for conflict, as both administrative and military capacities can shape the calculus to rebel against the state (Hendrix and Young, 2014). Hanson and Sigman (2021) use a variety of existing measures for extractive, coercive, and administrative state capacity, and show these three dimensions are linked to each other and mutually supportive. I use the general purpose measure of state capacity provided by Hanson and Sigman (2021), estimated using Bayesian latent variable analysis. Furthermore, the polity scores as an indicator of the level of democracy, the gross domestic product (GDP) per capita, and the population data are included in the analyses (Gleditsch, 2002).

Organisational attributes of armed groups can influence the success of mobilisation. However, it is essential to note that attributes that imply strength are endogenous, as information on them is typically collected retrospectively after successful mobilisation. In other words, groups that have successfully mobilised and gained strength over time are usually labelled as strong, and tracking changes over time is often challenging due to the scarcity of acces-

sible information. Nevertheless, some groups may exhibit a greater propensity to mobilise and escalate when formed. For instance, a group predominantly formed by experienced ex-combatants or foreign fighters may possess higher capabilities and strength at the initial stage, compared to groups formed by inexperienced militants. Following Malone (2021), I utilise a binary variable to indicate whether the initial members of the group are primarily foreign fighters or ex-combatants. Moreover, I utilise information from AGD on the ways groups emerge, taking into account splinter groups, merger groups, political parties turning violent and violent actors turning against the state. In all four cases, the baseline propensity for escalation can differ, as each suggests varying levels of available capacity, resources, and popular support.

Certain attributes may also bolster mobilisation by expanding the recruitment pool or individuals' willingness to join the organisation in its early stages. Armed groups emerging out of starker incompatibilities with the government may mobilise more quickly than others. To capture such dynamics, albeit limited to available information, I control for two binary indicators showing whether a group has ethno-national identity and whether a group has religious ideology, using data from AGD (Malone, 2022b). The summary statistics are presented in Table 4.1.

Statistic	N	Mean	St. Dev.	Min	Max
State share of ISPs	1,922	0.356	0.272	0.000	1.000
Mobile phones per 100 people	1,917	33.149	36.333	0.000	175.873
Number of ISP companies	1,922	3.520	1.438	1	7
Population (log)	1,915	3.217	1.119	0.005	5.119
GDP per capita (log)	1,703	11.377	1.614	7.520	13.929
Military expenditures (log)	1,701	13.143	1.694	6.909	16.048
State capacity	1,876	−0.342	0.765	−2.310	1.204
Judicial constraints on the executive index	1,915	0.418	0.260	0.006	0.863
Polity score	1,869	0.681	4.962	−9	9
Veteran members	1,922	0.287	0.452	0	1
Ethnonational	1,922	0.423	0.494	0	1
Religious	1,922	0.284	0.451	0	1

Table 4.1: Summary statistics

4.4.4 Modelling Mobilisation

I model the duration of mobilisation, which I define as the time from group formation to exceeding civil conflict threshold of 25 battle-deaths, using Cox proportional hazard models. I prefer a semi-parametric model since the theoretical arguments do not suggest a specific functional form for the baseline hazard, while the effect of the independent variable on the hazard function is the main focus.

The unit of analysis is the armed group vs. state dyad-year, and the data structure represents a counting process to include time-varying covariates. A dyad-year entry is present starting from the year the armed group formed, and observations are included until the group escalates the fight into civil conflict, or until the group stops using political violence. Groups that had not passed the threshold but were still active at the end of the time scope are right-censored, while groups formed before the start of the time scope are left-censored. However, the ages of groups for left-censored observations have been taken into account. The study period is limited to the overlap between the AGD and TOSCO datasets, covering between 2000 and 2012. There are 203 armed groups in the sample, operating in 37 countries, comprising a total of 1922 dyad-year observations.

An armed group can deescalate a civil conflict, and at some point in the future the conflict can reoccur again. I did not include such second and subsequent conflicts that an armed group experiences, considering the dynamics of further escalation would be of a different nature, which are not necessarily relevant to the theory presented here. For example, a ceasefire or a peace agreement can be made after an episode of civil conflict without disarming and demobilising militants, and such conflicts can reoccur without a new recruitment campaign.

To allow for different baseline hazards by different types of group formation, I use a stratified model using a categorical variable with five levels: new group, splinter group, merger group, political party turning violent, and other armed actors (such as militias, tribal movements, criminal organisations) turning against the state. The covariates included in the model are time variant, except group-level attributes. Since observations are nested by

country and several covarites are at the country-year level, robust standard errors clustered at the country level are used in all models. To test *H1a*, I use an interaction term with the state share of ISPs and network penetration, with the latter measured as mobile phone subscriptions per 100 people.

4.5 Analysis

Using the data described in the previous section, I estimate Cox proportional hazard models, regressing the duration of mobilisation on the state share of ISPs and other covariates. Table 4.2 presents two regression specifications, along with a replication using a subset of the data. Here, negative coefficients show a decrease in the hazard of a rebel group escalating into civil war, thus longer mobilisation duration. Model 1 is the main specification with all covariates and yields results in support of hypothesis 1. The exponentiated value of the coefficient estimate for the state share of ISPs is 0.129, indicating an 87% decrease in the baseline hazard rate when a state has full share of ISP companies compared to states with no share. In other words, the escalation into civil conflict takes a substantively longer time when the state has full ownership over telecommunication infrastructure. This change in hazard rate is visualised with survival curves in Figure 4.3, taking reference a newly formed religious group that is not formed primarily by veteran members and mean values of other covariates. The y-axis shows the predicted probability of survival at a given dyad-year since the formation of the rebel group, indicated on the x-axis. The lines show the predicted values using different values of state share of ISPs. A higher probability of survival indicates a longer duration of mobilisation, which means that a longer amount of time is required for escalation into civil conflict.

Model 2 introduces an interaction term with the state share of ISPs and network penetration, measured as mobile phone subscriptions per 100 people. The coefficient of the interaction term is statistically significant and negative, supporting hypothesis 1a. This in-

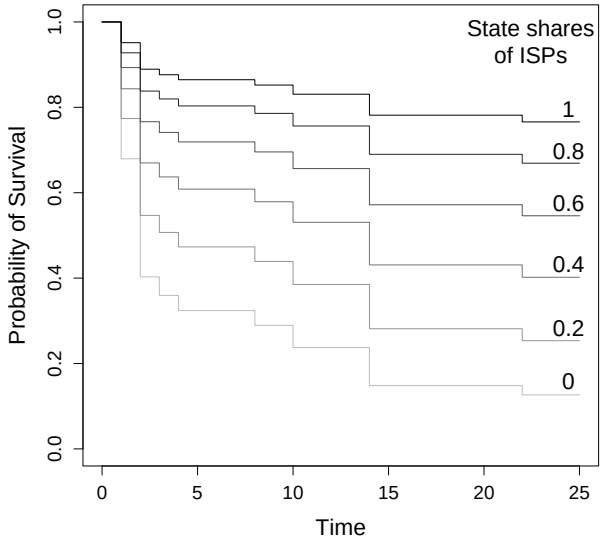


Figure 4.3: Survival curves for varying levels of state share of ISPs (Model 1, full sample)

dicates that the decrease in the baseline hazard rate associated with the state share of ISPs becomes larger in magnitude as network penetration increases. This relationship is visualised in Figure 4.4 with survival curves using the same reference values as in Figure 4.3, except the interaction term: mobile phone subscriptions per 100 people. The five plots show replications using minimum, maximum, and quartile values of network penetration in the sample. As the network penetration increases, the decrease in the hazard rate inflicted by higher state share of ISPs gets substantively larger.

AGD includes all armed groups that have used political violence at least once, but throughout history some groups were formed only for a specific attack or for a very brief period of time, such as one day or one week (Malone, 2022b). To address this issue, the dataset provides an indicator –*sustained violence*– which identifies groups associated with multiple violent incidents. While we cannot definitively confirm whether these groups had the intention of mobilisation from the beginning, their inclusion might introduce some bias in the results. Therefore, Models 1 and 2 are replicated using a subset including only groups with sustained violence, presented in the right two columns of Table 4.2. The results are similar to those with full sample.

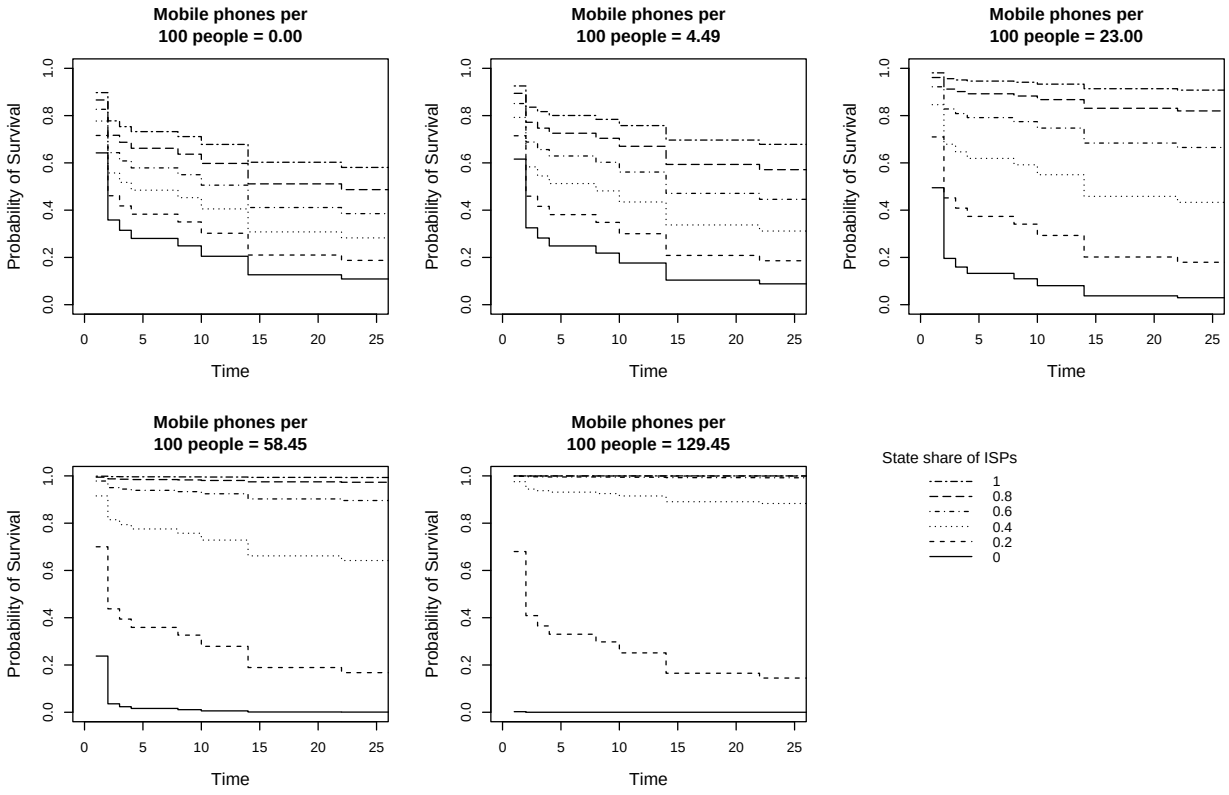


Figure 4.4: Survival curves for varying levels of state share of ISPs, grouped by minumum, maximum and quartile values of mobile phone subscriptions per 100 people (Model 2, full sample)

	Full sample		*Sustained violence* subset	
	Model 1	Model 2	Model 1	Model 2
Share of state	−2.047***	−1.406**	−2.020***	−1.411**
	(0.696)	(0.687)	(0.655)	(0.656)
Share of state × mobile phones		−0.095*		−0.085*
		(0.057)		(0.048)
Mobile phones per 100 people	−0.005	0.020	−0.004	0.019
	(0.006)	(0.014)	(0.007)	(0.012)
Number of ISP companies	−0.228	−0.211	−0.243	−0.230
	(0.163)	(0.163)	(0.161)	(0.161)
Population (log)	−0.431	−0.586	−0.490	−0.619**
	(0.354)	(0.360)	(0.314)	(0.312)
GDP per capita (log)	0.146	0.312	0.254	0.406
	(0.285)	(0.287)	(0.262)	(0.267)
Military expenditures (log)	0.028	0.001	0.033	0.002
	(0.167)	(0.153)	(0.168)	(0.156)
State capacity	−1.071***	−1.109***	−1.054***	−1.089***
	(0.338)	(0.326)	(0.345)	(0.333)
Judicial constraints on the executive index	−0.286	−0.291	−0.651	−0.660
	(0.844)	(0.871)	(0.893)	(0.933)
Polity score	0.051	0.057	0.061	0.065
	(0.045)	(0.044)	(0.041)	(0.040)
Veteran members	1.197**	1.256***	0.988**	1.065**
	(0.493)	(0.487)	(0.453)	(0.453)
Ethnonationalist	−0.222	−0.255	−0.349	−0.374
	(0.218)	(0.212)	(0.251)	(0.243)
Religious	1.495***	1.627***	1.269**	1.394***
	(0.476)	(0.460)	(0.497)	(0.486)
Concordance	0.783	0.800	0.748	0.774
Concordance SE	0.055	0.049	0.063	0.054
AIC	243.951	243.840	235.339	235.349
R^2	0.021	0.022	0.021	0.023
Num. events	41	41	41	41
Num. obs.	1563	1563	1231	1231

$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.
Errors are clustered at country level.
Sustained violence subset limits the sample to the armed groups associated with multiple incidents of political violence.
All models do not violate proportional hazard assumption. All variables do not individually violate it, except *religious* group indicator.

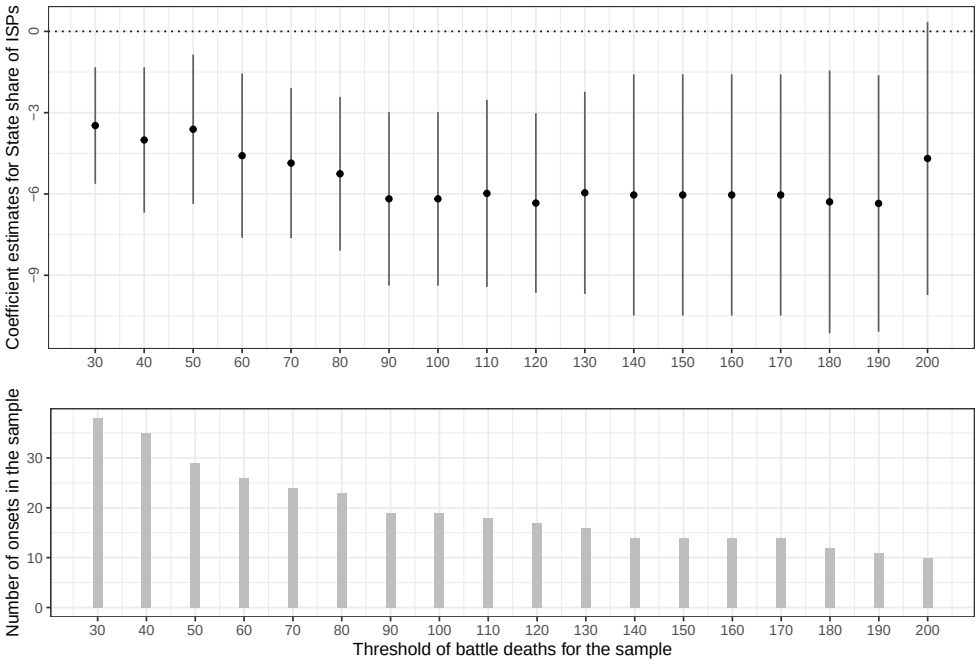
Table 4.2: Cox proportional hazard models

A key concept in mobilisation is the onset of civil conflict, which is operationalised using a threshold of 25 battle deaths. While this threshold is reasonable and necessary for identifying occurrences of civil conflict, it may also be considered arbitrary, since one less casualty in a year can leave out a dyad out of the civil conflict datasets. Therefore, to increase confidence in the results, Model 1 is replicated with varying thresholds of battle deaths considered for civil war onset, ranging from 30 to 200. The results are presented in Figure 4.5, where the number of conflict onsets left in the sample is shown on the panel below, with the x axis showing the number of battle deaths used as a threshold in each replication. The panel above in Figure 4.5 presents estimated coefficients for each replication, with each corresponding sample, including 0.95 confidence intervals.[11] As the threshold increases, the number of onsets in the sample naturally decreases, increasing the standard errors, but this robustness analysis overall shows that the findings are not driven by the choice of battle deaths threshold.

Another concern is the potential endogeneity between main variables of interest, state share of ISPs and mobilisation duration, as well as the other covariates used in the model. It is plausible that gaining control over telecommunications might trigger the processes discussed in the theory section concurrently. However, credibly claiming a causal effect in the observational setting presented here is not viable, even with time lags of independent variables, due to the potential presence of anticipation effects. Nevertheless, I replicate Table 4.2 using time-lagged values of the independent variables for one year. This approach reduces the time scope by one year and the number of onsets in the sample from 41 to 28. Consequently, the coefficient for the state share of ISPs becomes statistically insignificant, while still indicating a negative direction. Notably, the coefficient for the interaction term in Model 2 using sustained violence sample remains statistically significant at the 0.1 level (see Appendix 4.B).

Moreover, while I consider ownership to be the most evident form of control, in some cases owners of telecommunication companies may have informal links to the government elite, thus

[11] Design of this figure is inspired by Weidmann (2016).



Below histogram shows the number of onsets left in the sample as the battle-deaths threshold of civil conflict is increased. Above, the coefficient estimates for *state share of ISPs* for each corresponding sample are shown, with 0.95 confidence intervals.

Figure 4.5: Estimated coefficients for the main independent variable using samples with increasing thresholds for battle-deaths

may be more likely to provide support or assistance to the government regarding monitoring of communications. While it is difficult to identify those links, domestic owners might have a higher likelihood of having connections to the government compared to international owners. However, it is important to note that domestic ownership does not automatically imply political alignment with the government elite. To explore the implications of local ownership, I replicate Table 4.2 using domestic shares of ISPs as the independent variable instead of state shares. While using domestic ownership accounts for the possibility of local owners having connections to the government, it might not entirely exclude local owners with no such affiliations. Consequently, the results provide less conclusive support for the notion of control through domestic ownership. The coefficients for domestic shares of ISPs are smaller, with higher standard errors, but they remain statistically significant at the 0.1 level. However, the coefficient for the interaction of domestic shares and network penetration yields

statistically insignificant results with the full sample (see Appendix 4.C).

In the analyses, both state-level and rebel group-level attributes are controlled for, and clustered standard errors at the country level are used due to the nested structure of the data. Additionally, to gain further insights at the country level, I conduct a country-level analysis estimating the probability of conflict onset. This approach uses a time series cross-sectional setting with a binary dependent variable, which is equivalent to grouped duration data (Beck, Katz and Tucker, 1998). I use logistic regression models to estimate the probability of conflict onset, using state share of ISPs as the main independent variable. I control for variables that are associated with civil conflict in the existing literature. In addition to the country-level control variables used in the main set of models, I control for the fraction of the population that is politically excluded from the power, using information from the EPR dataset (Vogt et al., 2015). I also use a binary variable to indicate the presence of any other ongoing conflict in a country-year. To account for time trends, I use the time since the last onset, and squared and cubic terms of it (Carter and Signorino, 2010). The results do not show a statistically significant relationship between the probability of conflict onset in a country and the state share of ISP companies at the country level (see Appendix 4.D).

4.6 Discussion and Conclusion

This study investigates an overlooked aspect of communication technologies and conflict: the varying ability of states to exploit communication technologies for surveillance in order to prevent armed groups from escalating violence into a civil conflict. The assumption that states have complete control over the telecommunication infrastructure is very strong and unlikely to be true. Instead, this study takes a more nuanced approach and considers control as a function of ownership of telecommunication companies. Findings reveal that state ownership of ISP companies is associated with a longer duration of mobilisation for armed groups. This research contributes to the existing literature on the relationship between ICTs and armed

conflict, and it also sheds light on the interplay between state capacity, surveillance, and repression.

However, several limitations should be acknowledged. First, the sample used in the study is geographically and temporally restricted, limiting what can be inferred from the results. Expanding the coverage of existing datasets and developing new measures for state control over telecommunications would help us better understand the link between state surveillance and armed mobilisation. Second, while this chapter focuses exclusively on surveillance regarding the potential effects of control over telecommunications on the duration of armed mobilisation, empirically testing this mechanism is not possible with the available data.

State surveillance and the use of intelligence to counter uprisings are of significant importance for research, but this area of enquiry is hampered by the lack of available data due to the very nature of the phenomenon. However, surveillance is not new to history, and digital surveillance represents an evolution of long-standing strategies that governments have employed (Davenport, 2007). Therefore, historical accounts hold considerable theoretical value in understanding contemporary questions related to this subject.

In the future, states may continue to pursue control over telecommunications, albeit with changing forms and methods. Advances in technology and the growing international surveillance industry could enable more states to monitor telecommunications without relying on telecommunication network companies. Additionally, states are increasingly imposing regulations on international telecommunications and social media companies, compelling them to share data and respond to information requests from authorities. While recent advances in telecommunication technologies made it increasingly difficult for states to build, run, and maintain their own network without the involvement of private companies, the high costs of building an infrastructure keep states engaged in this realm. Many states are subsidising the roll-out of the fifth-generation (5G) mobile network infrastructure to help private companies with the very high costs, considering the promising economic returns (CSIS, 2021; European 5G Observatory, 2021; Grijpink et al., 2018; Guilford, 2019; Zhou, 2019).

Nevertheless, actors involved in conflicts adapt to new challenges over time and constantly seek new opportunities. In certain cases, we may witness a shift from shutting off communications out of fear of uprisings to keeping information channels open to identify dissenters and monitor them, or manipulating the information sphere in order to influence public opinion (Gunitsky, 2015). Future research can focus on exploring the various strategies within the repertoire of digital repression and examine the conditions under which states resort to such measures.

Appendix 4.A Correlation matrix of independent variables

	State share of ISPs	Mobile phones per 100 people	Number of ISP companies	Population (log)	GDP per capita (log)	Military expenditures (log)	State capacity	Judicial constraints on the executive index	Polity score	Veteran members	Ethnonational	Religious
State share of ISPs	1	−0.290	−0.540	−0.240	−0.209	−0.051	−0.072	−0.286	−0.278	−0.009	0.038	0.091
Mobile phones per 100 people	−0.290	1	0.210	0.246	0.553	0.575	0.492	0.281	0.174	−0.112	−0.120	0.138
Number of ISP companies	−0.540	0.210	1	0.477	0.226	0.059	−0.204	0.276	0.384	0.041	0.098	−0.154
Population (log)	−0.240	0.246	0.477	1	0.828	0.664	0.071	0.295	0.207	−0.181	0.104	0.037
GDP per capita (log)	−0.209	0.553	0.226	0.828	1	0.902	0.434	0.335	0.119	−0.247	−0.054	0.163
Military expenditures (log)	−0.051	0.575	0.059	0.664	0.902	1	0.464	0.179	−0.076	−0.193	−0.087	0.202
State capacity	−0.072	0.492	−0.204	0.071	0.434	0.464	1	0.554	0.095	−0.213	−0.165	0.329
Judicial constraints on the executive index	−0.286	0.281	0.276	0.295	0.335	0.179	0.554	1	0.443	−0.122	−0.029	0.129
Polity score	−0.278	0.174	0.384	0.207	0.119	−0.076	0.095	0.443	1	−0.078	0.156	−0.169
Veteran members	−0.009	−0.112	0.041	−0.181	−0.247	−0.193	−0.213	−0.122	−0.078	1	0.041	0.066
Ethnonational	0.038	−0.120	0.098	0.104	−0.054	−0.087	−0.165	−0.029	0.156	0.041	1	−0.227
Religious	0.091	0.138	−0.154	0.037	0.163	0.202	0.329	0.129	−0.169	0.066	−0.227	1

Table 4.3: Correlation matrix

Appendix 4.B Lagged values of the independent variables

	Full sample		*Sustained violence* subset	
	Model 1	Model 2	Model 1	Model 2
Share of state$_{t-1}$	−1.464	−0.784	−1.379	−0.772
	(0.973)	(1.019)	(0.919)	(0.969)
Share of state$_{t-1}$ × mobile phones$_{t-1}$		−0.151		−0.134*
		(0.096)		(0.082)
Mobile phones per 100 people$_{t-1}$	−0.013	0.026	−0.013	0.023
	(0.008)	(0.025)	(0.008)	(0.023)
Number of ISP companies$_{t-1}$	−0.124	−0.105	−0.099	−0.090
	(0.190)	(0.187)	(0.194)	(0.191)
Population (log)$_{t-1}$	−0.751*	−0.930**	−0.798*	−0.931**
	(0.435)	(0.423)	(0.441)	(0.432)
GDP per capita (log)$_{t-1}$	0.337	0.509	0.386	0.548
	(0.457)	(0.430)	(0.457)	(0.434)
Military expenditures (log)$_{t-1}$	0.042	0.054	0.073	0.065
	(0.252)	(0.239)	(0.254)	(0.244)
State capacity$_{t-1}$	−1.352***	−1.406***	−1.279**	−1.329***
	(0.495)	(0.478)	(0.521)	(0.503)
Judicial constraints on the executive index$_{t-1}$	0.849	0.897	0.682	0.704
	(0.871)	(0.846)	(0.943)	(0.909)
Polity score$_{t-1}$	0.062	0.065	0.066	0.066
	(0.050)	(0.051)	(0.054)	(0.055)
Veteran members	1.108**	1.221**	0.899*	1.046**
	(0.538)	(0.519)	(0.491)	(0.472)
Ethnonationalist	0.139	0.150	0.155	0.147
	(0.382)	(0.365)	(0.379)	(0.358)
Religious	2.447***	2.596***	2.298***	2.399***
	(0.613)	(0.624)	(0.648)	(0.649)
Concordance	0.814	0.827	0.786	0.808
Concordance SE	0.056	0.044	0.064	0.048
AIC	165.536	164.853	160.065	159.747
R^2	0.020	0.022	0.020	0.022
Num. events	28	28	28	28
Num. obs.	1429	1429	1147	1147

$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.
Errors are clustered at country level.
Sustained violence subset limits the sample to the armed groups associated with multiple incidents of political violence.
All models do not violate proportional hazard assumption. All variables do not individually violate it, except *religious* group indicator.

Table 4.4: Replication of Table 4.2 with lagged values (1 year) of independent variables

Appendix 4.C Domestic shares of ISPs as the independent variable

	Full sample		*Sustained violence* subset	
	Model 1	Model 2	Model 1	Model 2
Domestic shares of ISPs	−1.106*	−0.631	−1.120*	−0.678
	(0.636)	(0.627)	(0.590)	(0.597)
Domestic shares × mobile phones		−0.074		−0.069*
		(0.046)		(0.037)
Mobile phones per 100 people	−0.004	0.023	−0.004	0.022
	(0.006)	(0.016)	(0.007)	(0.014)
Number of ISP companies	−0.191	−0.202	−0.211	−0.228
	(0.176)	(0.188)	(0.178)	(0.190)
Population (log)	−0.497	−0.502	−0.523	−0.527
	(0.362)	(0.372)	(0.331)	(0.340)
GDP per capita (log)	0.356	0.494	0.436*	0.568**
	(0.262)	(0.305)	(0.243)	(0.287)
Military expenditures (log)	−0.068	−0.153	−0.056	−0.135
	(0.176)	(0.194)	(0.174)	(0.188)
State capacity	−1.187***	−1.240***	−1.159***	−1.215***
	(0.317)	(0.306)	(0.327)	(0.321)
Judicial constraints on the executive index	−0.040	0.147	−0.416	−0.260
	(0.802)	(0.783)	(0.844)	(0.821)
Polity score	0.049	0.044	0.058	0.056
	(0.047)	(0.047)	(0.041)	(0.041)
Veteran members	1.214**	1.238***	1.000**	1.033**
	(0.494)	(0.466)	(0.455)	(0.431)
Ethnonationalist	−0.198	−0.174	−0.327	−0.308
	(0.228)	(0.237)	(0.259)	(0.265)
Religious	1.424***	1.503***	1.172**	1.246***
	(0.474)	(0.425)	(0.491)	(0.440)
Concordance	0.779	0.790	0.731	0.759
Concordance SE	0.056	0.044	0.065	0.053
AIC	247.103	247.564	238.353	238.768
R^2	0.019	0.020	0.019	0.020
Num. events	41	41	41	41
Num. obs.	1563	1563	1231	1231

$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.
Errors are clustered at country level.
Sustained violence subset limits the sample to the armed groups associated with multiple incidents of political violence.
Domestic shares of ISPs and *religious* group variables individually violate the proportional hazard assumption. All models except Model 2 with full sample violate the assumption at 0.1 significance level.

Table 4.5: Replication of Table 4.2 with domestic shares of ISPs as independent variable

Appendix 4.D Country-level analysis

In this section of Appendix, I present a country-level analysis of state control over telecommunications and likelihood of conflict onset. The central argument of the study is that state control over telecommunications facilitates surveillance efforts and hinders militant mobilisation, leading to an increase in the duration of escalation into a civil conflict. Therefore, the unit of analysis in the main analyses is state vs. armed group dyad-year, and both state-level and rebel group-level attributes are controlled for in the models. Since the armed groups in the data are nested within countries, standard errors are clustered at the country level. Nevertheless, to gain further insight, I perform a country-level analysis to estimate the probability of conflict onset. This approach uses a time series cross-sectional setting with a binary dependent variable, which is equivalent to grouped duration data (Beck, Katz and Tucker, 1998). I use logistic regression models to estimate the probability of the onset of conflict, using the state share of ISPs as the main independent variable.

I control for variables that are associated with civil conflict in the existing literature. Specifically, I use GDP per capita, population and military expenditures in log scale, state capacity indicator form Hanson and Sigman (2021), and the polity score. Mobile phone subscriptions per 100 people and judicial constraints on the executive index from the V-dem data are also included in the models. These variables are the country-level control variables used in the main set of models. Additionally, I control for the fraction of the population that is politically excluded from the power, using information from the EPR dataset (Vogt et al., 2015). Finally, I use a binary variable to indicate the presence of any other ongoing conflict in a country-year. To account for time trends, I use the time since the last onset, and squared and cubic terms of it (Carter and Signorino, 2010). Over the period between 2000-2012, there are 526 country-year observations from 41 countries, and 30 civil conflict onsets in the sample. Due to the missing values in some of the covariates, row-wise deletion leaves 440 observations with 25 onsets.

The results are presented in Table 4.6. The first model is the main specification with all covariates. The second model drops observations after the first onset in a country. Onsets before 2000 are not taken into account when identifying the first onsets, since doing so significantly reduces the number of observations to 95, across only 11 countries. Although the coefficients for the state share of ISPs are negative in both models, the results are statistically insignificant. In Models 3 and 4, I introduce the term interacting state share of ISPs with mobile subscriptions per 100 people. Similarly to Model 2, Model 4 here uses a sample where observations after the first onset are dropped. The results are similar to those of the first two models, yielding statistically insignificant estimates, including for the interaction term. Models 5 and 6 use the rare events logistic regression, since onsets constitute only 5.6% of the observations. This method introduces a bias correction procedure for small samples with rare observations of events, and it is especially useful when the number of observations is under a few thousand and the events are under about 5% (King and Zeng, 2001, p. 157). Model 6 includes the interaction term. The results are also statistically insignificant in these models. Overall, this robustness check suggests that there is no clear relationship between civil conflict onsets and state share of ISPs.

	Logit models				Rare events logit	
	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
Intecept	−4.622	−1.786	−4.897	−0.823	−4.341	−4.663
	(5.285)	(5.286)	(5.247)	(5.116)	(4.069)	(4.175)
Share of state	−1.194	−1.084	−0.992	−1.650	−0.867	−0.564
	(1.299)	(1.413)	(1.304)	(1.648)	(1.315)	(1.462)
Share of state × mobile phones			−0.017	0.064		−0.021
			(0.058)	(0.109)		(0.059)
Mobile phones per 100 people	0.007	−0.011	0.011	−0.027	0.007	0.013
	(0.011)	(0.018)	(0.015)	(0.043)	(0.012)	(0.017)
Number of ISP companies	−0.114	0.191	−0.111	0.171	−0.101	−0.097
	(0.241)	(0.391)	(0.242)	(0.399)	(0.249)	(0.249)
Population (log)	0.078	−0.394	0.051	−0.328	0.042	0.008
	(0.768)	(0.734)	(0.777)	(0.717)	(0.619)	(0.626)
GDP per capita (log)	−0.343	−0.287	−0.315	−0.362	−0.289	−0.256
	(0.736)	(0.861)	(0.746)	(0.849)	(0.567)	(0.573)
Military expenditures (log)	0.362	0.281	0.363	0.279	0.329	0.330
	(0.286)	(0.295)	(0.279)	(0.316)	(0.324)	(0.323)
State capacity	−1.529*	−1.019	−1.523*	−0.972	−1.392**	−1.384**
	(0.893)	(1.098)	(0.884)	(1.131)	(0.689)	(0.685)
Judicial constraints on the executive index	0.710	−1.938	0.648	−2.037	0.620	0.556
	(1.190)	(1.957)	(1.257)	(2.031)	(1.361)	(1.375)
Polity score	0.057	0.130	0.060	0.128	0.051	0.053
	(0.059)	(0.098)	(0.061)	(0.099)	(0.067)	(0.068)
Share of excluded population	−0.200	1.298	−0.198	1.341	−0.164	−0.155
	(0.999)	(1.171)	(0.990)	(1.225)	(0.926)	(0.927)
Existing conflict (binary)	0.820	0.457	0.822	0.468	0.799	0.794
	(0.698)	(0.833)	(0.698)	(0.843)	(0.498)	(0.499)
Time since last onset	0.108	−0.196	0.107	−0.210	0.102	0.099
	(0.135)	(0.307)	(0.135)	(0.309)	(0.150)	(0.150)
Time^2	−0.007	0.009	−0.007	0.009	−0.007	−0.007
	(0.008)	(0.015)	(0.008)	(0.015)	(0.009)	(0.009)
Time^3	0.120	−0.099	0.118	−0.095	0.128	0.123
	(0.113)	(0.208)	(0.113)	(0.209)	(0.152)	(0.152)
Right-censored after first onset	NO	YES	NO	YES	NO	NO
AIC	203.074	135.547	204.987	137.157	203.074	204.987
BIC	264.376	192.579	270.376	197.991	264.376	270.376
Log Likelihood	−86.537	−52.774	−86.494	−52.578	−86.537	−86.494
Deviance	173.074	105.547	172.987	105.157	173.074	172.987
Num. obs.	440	331	440	331	440	440

$^{***}p < 0.01$; $^{**}p < 0.05$; $^{*}p < 0.1$.

Errors are clustered at country level except for rare events logistic regressions.

Model 2 and 4 uses a sample where observations dropped after the first onset in a country. Onsets before 2000 are not taken into account since doing so significantly reduces the number of observations (to a total of 95 observations across 11 countries).

Table 4.6: Country-level analysis: Logistic regressions on civil conflict onset

Chapter 5

Conclusion

This thesis advances our understanding of the interplay between information and communication technologies and conflict dynamics, and sheds light on how conflict actors strategically adapt their approaches in response to the opportunities and challenges presented by communication technologies. Moreover, it makes valuable contributions to the existing literature on rebel targeting in civil wars, as well as state repression and surveillance. In the concluding chapter, I first provide an overview of the main findings and insights from the substantive chapters, followed by a discussion on their limitations. I then discuss the policy implications that my findings potentially suggest, and propose several directions for future research, aiming to expand and enhance the knowledge in this field.

5.1 Summary of the findings

The second chapter of the thesis considers communication technologies over a continuum from older technologies to modern ones, and explores deliberate targeting of telecommunication infrastructure by rebel groups for over a span of approximately four decades. Drawing on existing literature on rebel targeting, it argues that rebel groups target telecommunication infrastructure when they perceive a significant risk to their survival. This risk becomes

more significant when rebels confront military forces with enhanced capabilities to detect and target militants effectively. The findings underscore the crucial role of information in civil conflicts, particularly in situations where there are notable disparities in capabilities between opposing forces. In addition, it sheds light on the specific tendencies motivated by the ideology of the group in relation to target selection. Marxist-socialist groups, relying heavily on indoctrination and propaganda, demonstrate the highest propensity to target telecommunication infrastructure. Additionally, ethno-religious groups also exhibit a higher likelihood of targeting telecommunications compared to other groups. The chapter contributes to the existing literature on ICT and conflict and on rebel targeting, providing valuable insight into rebel group strategies and improving our understanding of target selection processes.

The third chapter provides insight into how the latest generations of communication technologies can potentially impact conflict dynamics. Focusing on a modern communication technology that is commercially available, the chapter explores how rebel groups can take advantage of it to improve information processing within their organisation and bolster their propaganda efforts. Specifically, it contends that the adoption of 3G communication technology can yield improvements in areas where rebels already utilise telecommunications to some degree, including in-group monitoring, indoctrination and propaganda, diffusion of skills and knowledge, real-time coordination, and intelligence gathering. The chapter then gives a detailed account of telecommunications and the civil war in Afghanistan, and demonstrates that the Taliban and the other insurgent groups are likely to be exploiting communication technologies for their benefit, despite the risk of being detected and targeted. The findings show that the introduction of 3G networks in areas with existing 2G networks is associated with an increase in insurgent violence. It is important to acknowledge that the findings do not necessarily generalise to all civil wars. The observed increase in violence in the Afghanistan case reflects an overall improvement in the organisational effectiveness of the rebels, and this improvement may result in different outcomes depending on the groups' aims and strategies. Overall, the chapter advances our understanding of the intricate relationship between

communication technologies and coordination and collective action within militant groups.

The fourth chapter turns to the state and explores the relationship between state control over telecommunications and the dynamics of conflict. In particular, it investigates whether digital surveillance by states hinders militant mobilisation and makes it difficult for armed groups to violently challenge the state. It links the control of companies with the ownership structure, and measures state control using state share of telecommunication companies. The chapter provides a detailed overview of how states can potentially exploit their control over ICT infrastructure. It argues that state control over telecommunication infrastructure facilitates surveillance efforts aimed at detecting potential uprisings and preemptively responding to challenges, thus impeding militant mobilisation and prolonging the duration of mobilisation process. In an analysis of African countries between 2000-2012, the findings indicate that in countries where the state shares of telecommunication network companies are higher, the duration between the formation of militant groups and the escalation into civil conflict tends to be longer. The chapter contributes to the existing literature on state capacity-repression nexus, militant mobilisation, and the interplay between ICTs and armed conflict.

5.2 Limitations

While the thesis provides important insights into the dynamics between conflict and communication technologies, several limitations must be acknowledged. First, the studies presented here use observational data, and the findings present correlational relationships rather than causality. Political violence and civil conflict may exhibit endogenous relationships, since violence itself can influence social outcomes, making it challenging to achieve causal identification. Although statistical remedies have been employed to account for unobserved confounders, what we can infer from the analyses may fall short of establishing a direct causal effect. An experimental setting is non-viable, particularly at the country or rebel group level. Nevertheless, the quantitative research designs applied in the chapters are one way among

several to test the theoretical propositions presented. Qualitative research can document important aspects of the relationships under study, exploring micro-mechanisms, such as how communication technologies are utilised by militants in particular cases.

Data availability and quality stand as important obstacles to overcome. The targeting of telecommunication infrastructure is potentially underreported in conflict event datasets. A significant portion (87%) of attacks on the telecommunication infrastructure consists of non-lethal attacks directed at facilities. Non-lethal events with relative insignificance can be overlooked by the media, especially in conflicts with numerous civilian and combatant casualties. For example, incidents in which cell phone towers are set on fire or destroyed with explosives, resulting in no injuries or deaths, are less likely to attract attention and appear in the news. Alternatively, comprehensive documentation of these attacks might be found within private companies that provide mobile communication services, as many of these infrastructures are privately owned. A second resource might be governments that have the organisational capacity to efficiently record these events despite the ongoing conflict.

The third and fourth chapters of the thesis propose potential mechanisms that are challenging to observe directly and require systematic data collection under difficult circumstances. While it is possible to collect traces of information on militant use of telecommunication technologies, gaining systematic insight into how they precisely utilise ICTs for within-group communication necessitates fieldwork among the militants, which poses unacceptable levels of risk to researchers. Similarly, in the context of Chapter 4, state surveillance is inherently a covert activity, and systematic data collection on digital or physical surveillance efforts is practically impossible. Although researchers can rely on investigative reports or statements from former security agents of states, these sources may not be sufficient for a comprehensive and systematic study. Furthermore, tracking the international trade of surveillance products is difficult, and existing reports often lack information on companies based in countries such as Russia or China, due to the lack of transparency. Lastly, the dataset used in Chapter 4 is confined to countries in Africa, and the generalisability of the

findings to other contexts remains untested. Expanding the research to other regions would be essential to validate the broader implications of the study's results.

5.3 Policy implications

Chapter 2 demonstrates that the telecommunication infrastructure can be systematically targeted in some civil conflicts. This can have direct and indirect consequences for the local population and can victimise civilians. Firstly, this type of violence hampers civilians' access to the telecommunication network, effectively disconnecting local populations. As a result, the information flow from affected communities regarding their needs for aid can be limited, journalists' access may be restricted, and incidents of violence against civilians or human rights abuses can remain concealed. Secondly, attacks on telecommunications can also result in the victimisation of officials or workers of telecommunication, radio, or TV companies operating in conflict-affected areas. The risk to these personnel should be carefully assessed when working in such environments.

Chapter 3 highlights that rebel groups can exploit new generations of communication technologies to enhance their organisational effectiveness, particularly in areas such as within-group coordination and propaganda. As with any technological advancement, modern communication technologies have the potential for both beneficial and harmful applications. Restricting the expansion of telecommunication networks in conflict-affected regions only due to potential risks would be imprudent, considering the significant benefits they can offer local populations. As discussed at length in Chapter 4, states can also exploit their control over telecommunications. Any party in a civil conflict would try to benefit from the opportunities offered by communication technologies, with the potential to victimise civilians. Implementing regulations to control and monitor the use of telecommunications might be perceived as a preventive measure to maintain public order and protect civilians, but governments should be held accountable for their actions on the basis of human rights. This balance can be

very difficult to achieve in practice, and the ongoing debate surrounding the trade-off between security and digital privacy is likely to continue in the future. Furthermore, improving regulations and control over the international trade of digital surveillance products may be beneficial. This approach would enable better tracking of such capabilities and may help the international community address potential human rights violations.

5.4 Directions for future research

Building upon the cross-sectional study presented in Chapter 2, future research could advance our understanding of the micro-mechanisms underlying attacks on telecommunication infrastructure by rebel groups in civil conflicts. A fruitful next step would be to conduct a disaggregated study, focusing on sub-national contexts to explore the spatial and temporal variation of these attacks. The link between the military capabilities of government forces and the targeting of telecommunications by rebels is related to battlefield dynamics, which point to contested territories rather than controlled areas by the parties of conflict. Therefore, territorial control can explain part of the spatial variation. Regarding temporal patterns, attacks on telecommunications might be more likely when there are large-scale military operations that threaten the survival of the rebel group. Multiple simultaneous attacks on telecommunications may aim to cut down networks in a large territory, potentially foreshadowing an escalation of violence. Rebel groups with Marxist-socialist or ethno-religious ideological orientations may be more likely to target telecommunications when they lack control over territory and do not possess access to mass communication channels. It is also worth looking at attacks on other types of infrastructure, such as food or water supplies or energy infrastructure. These are targeted by a larger number of rebel groups compared to telecommunications.[1]

[1]The same coding procedure used in Chapter 2 reveals that 105 out of 372 groups have targeted other types of infrastructure (including food and water supplies, utilities, bridge/car tunnels and highway/road/toll/traffic signals), while 46 of them had targeted telecommunications. Most of the groups that target telecommunications also target other types of infrastructure (START, 2021).

The new challenges facing rebels or governments in civil conflict force them to innovate and adapt new solutions. For example, more effective drone strikes by governments may compel rebels to hide or infiltrate civilian population more, and this on the other side may push governments to develop more precise targeting technologies. A similar concern and an interesting question would be the consequences of introducing a global wireless network with less or any physical infrastructure on the ground (e.g. satellite constellation projects of various tech-companies). It may cause rebels to be more violent against civilians in contested areas in a conflict, with concerns over denunciation.

Although Chapter 3 argues that modern communication technologies can be used by militants for within-group communications, we lack systematic evidence on how militants exactly use such technologies. While the risks and challenges of doing an ethnographic study among militants are obvious, interviews with ex-combatants may prove insightful for future studies. Such work would shed light on specific areas ICTs are being employed, and whether and how the diffusion of skills, monitoring of militants, and hierarchical feedback channels benefit from modern ICTs.

A substantial part of the internet usage is through social media and video streaming platforms, and search engines are also among the most visited websites on the internet. Such platforms use a variety of algorithms to improve and personalise user experience, or optimise targeted advertisements. Rebel groups are also increasingly using social media and the internet for propaganda and recruitment purposes (Loyle and Bestvater, 2019). Those algorithms in social media platforms have the potential to mediate the impacts of ICT on social outcomes, which may have implications that we are yet to understand (Gohdes, 2018).

Finally, future projects can examine different methods in the repertoire of digital repression. For instance, we know little about the use and implications of targeted digital repression methods within contentious politics, such as censorship or content removal. Furthermore, cross-national studies can complement existing sub-national studies that examine network shutdowns (Gohdes, 2020; Mustafa, 2023). A relatively recent trend among states is

the introduction of policies and regulations restricting social media and internet companies. While the extent and enforcement of such regulations may vary between countries, social media companies may also prefer to comply with some governments while resisting others. Future work can explore the logic and implications of such policies. In general, broadening the research agenda on the relationship between ICTs and conflict will further enrich our understanding and help inform more effective policies and responses in conflict-affected regions.

Bibliography

Adebisi, Sunday A; R Oyedeji and O Azeez (2015) Boko Haram insurgency in Nigeria: Defining, addressing and understanding its impact on telecommunication industry. *Economics and Management Research Projects: An International Journal* 5(1): 10–17.

Agubor, Cosmas K; Gloria A Chukwudebe and Onyebuchi C Nosiri (2015). Security challenges to telecommunication networks: An overview of threats and preventive strategies. In: 2015 International Conference on Cyberspace (CYBER-Abuja) , 124–129.

Aker, Jenny C and Isaac M Mbiti (2010) Mobile phones and economic development in Africa. *Journal of Economic Perspectives* 24(3): 207–232.

Akwaja, Chima (2012) Nigeria: Mobile operators cry out as terrorists bomb facilities. *AllAfrica* 6 September (https://allafrica.com/stories/201209060225.html).

Anadolu Ajansi (2015) 'Terör örgütü şantiyelerimize, yollarımıza saldırıyor'. *Anadolu Ajansi* 21 October (https://www.aa.com.tr/tr/turkiye/teror-orgutu-santiyelerimize-yollarimiza-saldiriyor/448973).

Anders, Therese (2020) Territorial control in civil wars: Theory and measurement using machine learning. *Journal of Peace Research* 57(6): 701–714.

Ankersen, Christopher and Mike Martin (2021) The Taliban, not the West, won Afghanistan's technological war. *MIT Technology Review* 23 August Accessed: 20.10.2021

(https://www.technologyreview.com/2021/08/23/1032459/afghanistan-taliban-war-technological-progress/).

Asal, Victor; Ken Cousins and Kristian Skrede Gleditsch (2015) Making ends meet: Combining organizational data in contentious politics. *Journal of Peace Research* 52(1): 134–138.

Asal, Victor; Brian J Phillips and R Karl Rethemeyer (2022) *Insurgent Terrorism: Intergroup Relationships and the Killing of Civilians*. New York: Oxford University Press.

Asal, Victor; Brian J Phillips, R Karl Rethemeyer, Corina Simonelli and Joseph K Young (2019) Carrots, sticks, and insurgent targeting of civilians. *Journal of Conflict Resolution* 63(7): 1710–1735.

Awad, Atif and Mohamed Albaity (2022) Ict and economic growth in Sub-Saharan Africa: Transmission channels and effects. *Telecommunications Policy* 46(8): 102381.

Bailard, Catie Snow (2015) Ethnic conflict goes mobile: Mobile technology's effect on the opportunities and motivations for violent collective action. *Journal of Peace Research* 52(3): 323–337.

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

Banks, Arthur S and Kenneth A Wilson (2021) *Cross-National Time-Series Data Archive*. Jerusalem, Israel: Databanks International (https://www.cntsdata.com/).

Barnett, David (2013) Al Furqan Brigades claim attack on satellite station in Cairo. *FDD's Long War Journal* 8 October (https://www.longwarjournal.org/archives/2013/10/al_furqan_brigades_claim_respo.php).

Bashir, Malali (2017) Taliban propaganda meets the Digital age. *RFE/RL* 10 July Accessed: 20.10.2021 (https://gandhara.rferl.org/a/taliban-propaganda/28606576.html).

Bazzi, Samuel and Christopher Blattman (2014) Economic shocks and conflict: Evidence from commodity prices. *American Economic Journal: Macroeconomics* 6(4): 1–38 (http://www.jstor.org/stable/43189938).

BBC (2010) Seized Somali media network 'must serve Islam'. *BBC* 20 September (https://www.bbc.co.uk/news/world-africa-11376013).

BBC (2012) Afghan Taliban use phones for propaganda. *BBC* 30 March Accessed: 20.10.2021 (https://www.bbc.co.uk/news/world-asia-17563068).

BBC (2016) Taliban app removed from Google store. *BBC* 04 April Accessed: 20.10.2021 (https://www.bbc.co.uk/news/technology-35959534).

Beck, Nathaniel; Jonathan N Katz and Richard Tucker (1998) Taking time seriously: Time-series-cross-section analysis with a binary dependent variable. *American Journal of Political Science* 42(4): 1260–1288 (http://www.jstor.org/stable/2991857).

Bennett, Brian T (2018) *Understanding, assessing, and responding to terrorism : Protecting critical infrastructure and personnel (Second ed.).* Hoboken, NJ: John Wiley and Sons, Incorporated.

Berman, Eli; Jacob N Shapiro and Joseph H Felter (2011) Can hearts and minds be bought? The economics of counterinsurgency in Iraq. *Journal of Political Economy* 119(4): 766–819.

Blakely, Rhys (2005) Terrorists 'threaten' Iraq Mobile Operators. *The Times* 22 July (https://www.thetimes.co.uk/article/terrorists-threaten-iraq-mobile-operators-frnph63v6jt).

Boone, Jon (2011) Taliban target mobile phone masts to prevent tipoffs from Afghan civilians. *The Guardian* 11 November (https://www.theguardian.com/world/2011/nov/11/taliban-targets-mobile-phone-masts).

Botha, Anneli (2021) Prevention of terrorist attacks on critical infrastructure. In: Alex P Schmid (ed.) *Handbook of Terrorism Prevention and Preparedness*. The Hague: ICCT Press Publicationchapter 28, , 841–870.

Buhaug, Halvard; Mihai Croicu, Hanne Fjelde and Nina von Uexkull (2021) A conditional model of local income shock and civil conflict. *The Journal of Politics* 83(1): 354–366.

Buhaug, Halvard; Scott Gates and Päivi Lujala (2009) Geography, rebel capability, and the duration of civil conflict. *Journal of Conflict Resolution* 53(4): 544–569.

Carter, David B and Curtis S Signorino (2010) Back to the future: Modeling time dependence in binary data. *Political Analysis* 18(3): 271–292.

Christensen, Darin and Francisco Garfias (2018) Can you hear me now? How communication technology affects protest and repression. *Quarterly Journal of Political Science* 13(1): 89–117.

CIESIN (2018) *Gridded Population of the World, Version 4 (GPWv4): Population Density, Revision 11*. Center for International Earth Science Information Network - Columbia University. Palisades, NY: NASA Socioeconomic Data and Applications Center (SEDAC).

Cinelli, Carlos; Jeremy Ferwerda and Chad Hazlett (2020) Sensemakr: Sensitivity analysis tools for OLS in R and Stata. R package Version 0.1.3.

Cinelli, Carlos and Chad Hazlett (2020) Making sense of sensitivity: Extending omitted variable bias. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)* 82(1): 39–67.

Clark, Kate (2020) One land, two rules (11): Delivering public services in insurgency-affected districts - A synthesis report. *Afghanistan Analysts Network* 06 May Accessed: 20.10.2021 (https://www.afghanistan-analysts.org/en/reports/war-and-peace/one-land-two-rules-11-delivering-public-services-in-insurgency-affected-districts-a-synthesis-report/).

Clark, Kate and Jelena Bjelica (2018) One Land, Two Rules (1): Service delivery in insurgent-affected areas, an introduction. *Afghanistan Analysts Network* 06 December Accessed: 20.10.2021 (https://www.afghanistan-analysts.org/en/reports/economy-development-environment/one-land-two-rules-1-service-delivery-in-insurgent-affected-areas-an-introduction/).

Cohen, Dara Kay and Ragnhild Nordås (2014) Sexual violence in armed conflict: Introducing the SVAC dataset, 1989-2009. *Journal of Peace Research* 51(3): 418–428.

Cook, Scott J and Nils B Weidmann (2021) Race to the bottom: Spatial aggregation and event data. *Working Paper August 24, 2021*.

Coppedge, Michael; John Gerring, Carl Henrik Knutsen, Staffan Lindberg, Jan Teorell, David Altman, Michael Bernhard, Agnes Cornell, M Steven Fish, Lisa Gastaldi, Haakon Gjerløw, Adam Glynn, Sandra Grahn, Allen Hicken, Katrin Kinzelbach, Kyle L Marquardt, Kelly McMann, Valeriya Mechkova, Pamela Paxton, Daniel Pemstein, Johannes von Römer, Brigitte Seim, Rachel Sigman, Svend-Erik Skaaning, Jeffrey Staton, Eitan Tzelgov, Luca Uberti, Yi ting Wang, Tore Wig and Daniel Ziblatt (2022) V-Dem codebook v12. Technical report. Varieties of Democracy (V-Dem) Project (https://www.v-dem.net/documents/1/codebookv12.pdf).

CSIS (2021) Accelerating 5G in the United States. Accessed: 16.07.2023 (https://www.csis.org/analysis/accelerating-5g-united-states).

Cunningham, David E; Kristian Skrede Gleditsch and Idean Salehyan (2009) It takes two: A dyadic analysis of civil war duration and outcome. *Journal of Conflict Resolution* 53(4): 570–597.

Cunningham, David E; Kristian Skrede Gleditsch and Idean Salehyan (2013) Non-state actors in civil wars: A new dataset. *Conflict Management and Peace Science* 30(5): 516–531.

Daily Balochistan Express (2018) Six labourers shot dead in Kharan. *Daily Balochistan Express* 05 May (https://bexpress.com.pk/2018/05/six-labourers-shot-dead-in-kharan).

Davenport, Christian (2007) State repression and political order. *Annual Review of Political Science* 10(1): 1–23.

Daxecker, Ursula (2017) Dirty hands: Government torture and terrorism. *The Journal of Conflict Resolution* 61(6): 1261–1289 (http://www.jstor.org/stable/26363927).

de Castro Leal, Débora; Max Krüger, Kaoru Misaki, David Randall and Volker Wulf (2019). Guerilla warfare and the use of new (and some old) technology: Lessons from FARC's armed struggle in Colombia. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems CHI '19 , 1–12. New York. Association for Computing Machinery.

De la Calle, Luis (2017) Compliance vs. Constraints: A theory of rebel targeting in civil war. *Journal of Peace Research* 54(3): 427–441.

DeSombre, Winnona; Lars Gjesvik and Johann Ole Willers (2021) Surveillance technology at the fair: Proliferation of cyber capabilities in international arms markets. Technical report. Atlantic Council.

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

Dimitrov, Martin K and Joseph Sassoon (2014) State Security, Information, and Repression: A Comparison of Communist Bulgaria and Ba'thist Iraq. *Journal of Cold War Studies* 16(2): 3–31.

Doctor, Austin C and James I Walsh (2021) The coercive logic of militant drone use. *Parameters* 51(2).

Drake, CJ M (1998) The role of ideology in terrorists' target selection. *Terrorism and Political Violence* 10(2): 53–85.

Drakos, Konstantinos and Andreas Gofas (2006) The devil you know but are afraid to face: Underreporting bias and its distorting effects on the study of terrorism. *Journal of Conflict Resolution* 50(5): 714–735.

Dube, Oeindrila and Juan F Vargas (2013) Commodity price shocks and civil conflict: Evidence from Colombia. *The Review of Economic Studies* 80(4): 1384–1421.

Edmond, Chris (2013) Information manipulation, coordination, and regime change. *The Review of Economic Studies* 80(4): 1422–1458.

European 5G Observatory (2021) Public 5G funding. Accessed: 16.07.2023 (https://5gobservatory.eu/public-funding-of-5g-rd-including-trials/).

Fearon, James D (1995) Rationalist explanations for war. *International Organization* 49(3): 379–414 (http://www.jstor.org/stable/2706903).

Fearon, James D and David D Laitin (2003) Ethnicity, insurgency, and civil war. *The American Political Science Review* 97(1): 75–90.

Feldstein, Steven (2019) The global expansion of AI surveillance. Technical report. Carnegie Endowment for International Peace.

Feldstein, Steven (2022) Government internet shutdowns are changing. How should citizens and democracies respond? Technical report. Carnegie Endowment for International Peace.

Fjelde, Hanne; Lisa Hultman and Sara Lindberg Bromley (2016) Offsetting losses: Bargaining power and rebel attacks on peacekeepers. *International Studies Quarterly* 60(4): 611–623.

Fong, Christian; Chad Hazlett and Kosuke Imai (2018) Covariate balancing propensity score for a continuous treatment: Application to the efficacy of political advertisements. *The Annals of Applied Statistics* 12(1): 156–177.

Fong, Christian; Marc Ratkovic, Kosuke Imai Chad Hazlett, Xiaolin Yang and Sida Peng (2021) CBPS: R package for covariate balancing propensity score. Available at the Comprehensive R Archive Network (CRAN): https://CRAN.R-project.org/package=CBPS.

Fortna, Virginia Page; Nicholas J Lotito and Michael A Rubin (2018) Don't bite the hand that feeds: Rebel funding sources and the use of terrorism in civil wars. *International Studies Quarterly* 62(4): 782–794.

Fortna, Virginia Page; Nicholas J Lotito and Michael A Rubin (2022) Terrorism in armed conflict: New data attributing terrorism to rebel organizations. *Conflict Management and Peace Science* 39(2): 214–236.

Freedom House (2013) Publication archives. (https://freedomhouse.org/reports/publication-archives).

Freyburg, Tina and Lisa Garbe (2018) Authoritarian practices in the Digital age | Blocking the bottleneck: Internet shutdowns and ownership at election times in Sub-Saharan Africa. *International Journal of Communication* 12(0) (https://ijoc.org/index.php/ijoc/article/view/8546).

Freyburg, Tina; Lisa Garbe and Véronique Wavre (2023) The political power of internet business: A comprehensive dataset of telecommunications ownership and control (TOSCO). *The Review of International Organizations 18*: 573–600.

Galula, David (1964) *Counterinsurgency Warfare: Theory and Practice*. New York: Praeger.

Gates, Scott (2002) Recruitment and allegiance: The microfoundations of rebellion. *Journal of Conflict Resolution* 46(1): 111–130.

Gesch, Dean B; Kristine L Verdin and Susan K Greenlee (1999) New land surface digital elevation model covers the earth. *Eos, Transactions American Geophysical Union* 80(6): 69–70.

Gibbons-neff, Thomas and Mujib Mashal (2019) In Afghanistan's war and peace, Whatsapp delivers the message. *The New York Times* 26 October Accessed: 19.06.2023 (https://www.nytimes.com/2019/10/26/world/asia/afghanistan-whatsapp-taliban.html).

Giustozzi, Antonio (2007) *Koran, Kalashnikov and Laptop: The Neo-Taliban Insurgency in Afghanistan.* London: Hurst.

Giustozzi, Antonio (2019) *The Taliban at War: 2001 - 2018.* Oxford University Press.

Gleditsch, Kristian Skrede (2002) Expanded trade and GDP data. *Journal of Conflict Resolution* 46(5): 712–724.

GMacAskill, Ewen; Julian Borger, Nick Hopkins, Nick Davies and James Ball (2013) GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian.* 21 June (https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa).

Gohdes, Anita R (2015) Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research* 52(3): 352–367.

Gohdes, Anita R (2018) Studying the internet and violent conflict. *Conflict Management and Peace Science* 35(1): 89–106.

Gohdes, Anita R (2020) Repression technology: Internet accessibility and state violence. *American Journal of Political Science* 64(3): 488–503.

Gohdes, Anita R and Sabine C Carey (2017) Canaries in a coal-mine? What the killings of journalists tell us about future repression. *Journal of Peace Research* 54(2): 157 – 174.

Goldbaum, Christina and Safiullah Padshah (2023) The Taliban government runs on Whatsapp. There's just one problem. *The New York Times* 17 June Accessed: 19.06.2023 (https://www.nytimes.com/2023/06/17/world/asia/taliban-whatsapp-afghanistan.html).

Grijpink, Ferry; Alexandre Ménard, Halldor Sigurdsson and Nemanja Vucevic (2018) The road to 5G: The inevitable growth of infrastructure cost. Accessed: 16.07.2023 (https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost#/).

Groenewald, Yolandi (2017) Loophole used to spy on more than 70 000 phones in SA. *News24* 24 August Access date: 09 October 2022 (https://www.news24.com/fin24/tech/loophole-used-to-spy-on-more-than-70-000-phones-in-sa-20170824).

Guilford, Gwynn (2019) The tricky -and really expensive- business of building 5G. *Quartz* 28 September Accessed: 16.07.2023 (https://qz.com/1716218/to-build-out-5g-mobile-wireless-operators-must-spend-up-to-1-trillion-without-much-in-the-way-of-return).

Gunitsky, Seva (2015) Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics* 13(1): 42–54.

Gutiérrez-Sanín, Francisco and Elisabeth Jean Wood (2014) Ideology in civil war: Instrumental adoption and beyond. *Journal of Peace Research* 51(2): 213–226.

Hanson, Jonathan K and Rachel Sigman (2021) Leviathan's latent dimensions: Measuring state capacity for comparative political research. *The Journal of Politics* 83(4): 1495–1510.

Harbom, Lotta; Erik Melander and Peter Wallensteen (2008) Dyadic dimensions of armed conflict, 1946-2007. *Journal of Peace Research* 45(5): 697 – 710.

Hendrix, Cullen S (2010) Measuring state capacity: Theoretical and empirical implications for the study of civil conflict. *Journal of Peace Research* 47(3): 273–285.

Hendrix, Cullen S and Joseph K Young (2014) State capacity and terrorism: A two-dimensional approach. *Security Studies* 23(2): 329–363.

Hernández, Marianne Díaz; Felicia Anthonio, Sage Cheng and Alexia Skok (2022) Internet shutdowns in 2021: The return of digital authoritarianism. Accessed: 29.12.2022 (https://www.accessnow.org/internet-shutdowns-2021/).

Hiiraan Online (2018) Two employees of Somali telecom giant killed in Somali capital. *Hiiraan Online* 21 November (https://www.hiiraan.com/news4/2018/Nov/161211/two_employees_of_somali_telecom_giant_killed_in_somali_capital.aspx).

Howard, Philip N; Sheetal D Agarwal and Muzammil M Hussain (2011) When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review* 14(3): 216–232 (https://doi.org/10.1080/10714421.2011.597254).

Hultman, Lisa (2012) Attacks on civilians in civil war: Targeting the achilles heel of democratic governments. *International Interactions* 38(2): 164–181.

Humphreys, Macartan and Jeremy M Weinstein (2006) Handling and manhandling civilians in civil war. *The American Political Science Review* 100(3): 429–447.

Iacus, Stefano M; Gary King and Giuseppe Porro (2012) Causal inference without balance checking: Coarsened exact matching. *Political Analysis* 20(1): 1–24.

IDC (2023) Global smartphone shipments from 2009 to 2022 (in million units). Accessed: 16.07.2023 (https://www.statista.com/statistics/271491/worldwide-shipments-of-smartphones-since-2009/).

ITU (2008) ICT Data and Statistics (IDS). Accessed: 23.01.2023 (https://www.itu.int/ITU-D/ict/statistics/ict/index.html).

ITU (no date) ITU DataHub. Accessed: 23.01.2023 (https://datahub.itu.int/).

Kalyvas, Stathis N (2006) *The Logic of Violence in Civil War*. Cambridge: Cambridge University Press (Cambridge Studies in Comparative Politics).

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

Kann, Alyssa (2021) As the Taliban offensive gained momentum, so did its Twitter propaganda campaign. *Medium* 20 August Accessed: 20.10.2021 (https://medium.com/dfrlab/as-the-taliban-offensive-gained-momentum-so-did-its-twitter-propaganda-campaign-75021ba3082).

King, Gary and Langche Zeng (2001) Logistic regression in rare events data. *Political Analysis* 9(2): 137–163.

Kreft, Anne-Kathrin (2019) Responding to sexual violence: Women's mobilization in war. *Journal of Peace Research* 56(2): 220–233.

Little, Andrew T (2016) Communication technology and protest. *The Journal of Politics* 78(1): 152–166.

Loyle, Cyanne E and Samuel E Bestvater (2019) #rebel: Rebel communication strategies in the age of social media. *Conflict Management and Peace Science* 36(6): 570–590.

Lyall, Jason; Yuki Shiraito and Kosuke Imai (2015) Coethnic bias and wartime informing. *The Journal of Politics* 77(3): 833–848.

Mahmood, Rafat and Michael Jetter (2020) Communications technology and terrorism. *Journal of Conflict Resolution* 64(1): 127–166.

Malone, Iris (2021) The timing of militant violence onset. *Working Paper October, 2021*.

Malone, Iris (2022a) Economic shocks and militant formation. *Research & Politics* 9(2): 20531680221091436.

Malone, Iris (2022b) Unmasking militants: Organizational trends in armed groups, 1970-2012. *International Studies Quarterly* 66(3) sqac050.

Manacorda, Marco and Andrea Tesei (2020) Liberation technology: Mobile phones and political mobilization in Africa. *Econometrica* 88(2): 533–567.

Mann, Michael (1984) The autonomous power of the state : Its origins, mechanisms and results. *European Journal of Sociology / Archives Européennes de Sociologie / Europäisches Archiv für Soziologie* 25(2): 185–213.

Mann, Michael (2008) Infrastructural power revisited. *Studies in Comparative International Development 43*: 355–365.

Mare, Admire (2020) Internet shutdowns in Africa: State-ordered internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication* 14(0) (https://ijoc.org/index.php/ijoc/article/view/11494).

Masullo, Juan and Francis O'Connor (2020) PKK violence against civilians: Beyond the individual, understanding collective targeting. *Terrorism and Political Violence* 32(1): 77–99.

Meek, James Gordon (2015) Taliban urges supporters to use texting app to get Jihadi news. *ABC News* 01 June Accessed: 20.10.2021 (https://abcnews.go.com/International/taliban-urges-supporters-texting-app-jihadi-news/story?id=31444084).

Mir, Asfandyar and Dylan Moore (2019) Drones, surveillance, and violence: Theory and evidence from a US drone program. *International Studies Quarterly* 63(4): 846–862.

Morning Star (2005) Nepalese guerillas bomb state TV transmitter. *Morning Star* 19 May (https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:4G6J-SHC0-0159-S2RV-00000-00&context=1519360).

Morozov, Evgeny (2011) *The Net Delusion: The Dark Side of Internet Freedom*. Philadelphia, PA: PublicAffairs.

Mozur, Paul (2021) How the Taliban turned social media into a tool for control. *The New York Times* 20 August Accessed: 20.10.2021 (https://www.nytimes.com/2021/08/20/technology/afghanistan-taliban-social-media.html).

Mustafa, Fatima (2023) Can cellphone shutdowns stop terrorist violence? Evidence from Pakistan. *Terrorism and Political Violence* 35(2): 284–303.

NATO (2021) Defence expenditure of NATO countries (2013-2020). (https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210316-pr-2020-30-en.pdf).

Nickell, Stephen (1981) Biases in dynamic models with fixed effects. *Econometrica* 49(6): 1417–1426.

Nikzad, Khaled (2019) 220 telecom towers destroyed in eight months: ATRA. *TOLOnews* 26 November (https://tolonews.com/afghanistan/220-telecom-towers-destroyed-eight-months-atra).

NOAA (no date) Version 4 DMSP-OLS Nighttime Lights Time Series. Image and data processing by NOAA's National Geophysical Data Center. Defense Meteorological Satellite Program (DMSP) data collected by the US Air Force Weather Agency. Accessed: 25.05.2022 (https://www.ngdc.noaa.gov/eog/dmsp/downloadV4composites.html).

Parkinson, Sarah Elizabeth (2013) Organizing rebellion: Rethinking high-risk mobilization and social networks in war. *American Political Science Review* 107(3): 418–432.

Payab, Wais (2009). ICT Progress in Afghanistan. In: ITU Regional Cybersecurity Forum for Asia-Pacific. Hyderabad, India. Afghanistan National Data Center, Ministry of Communications and IT. Accessed: 20.10.2021 (https://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/payab-ict-af-cert-afghanistan-sept-09.pdf).

Pettersson, Therese (2020) UCDP dyadic dataset codebook v 20.1. (https://ucdp.uu.se/downloads/).

Pettersson, Therése and Magnus Öberg (2020) Organized violence, 1989-2019. *Journal of Peace Research* 57(4): 597–613.

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.

Polo, Sara MT (2020a) How terrorism spreads: Emulation and the diffusion of ethnic and ethnoreligious terrorism. *Journal of Conflict Resolution* 64(10): 1916–1942.

Polo, Sara MT (2020b) The quality of terrorist violence: Explaining the logic of terrorist target choice. *Journal of Peace Research* 57(2): 235–250.

Polo, Sara MT and Kristian Skrede Gleditsch (2016) Twisting arms and sending messages: Terrorist tactics in civil war. *Journal of Peace Research* 53(6): 815–829.

Privacy International (2016) The global surveillance industry. Technical report. Privacy International.

Privacy International (2017) Track, capture, kill: Inside communications surveillance and counterterrorism in Kenya. Technical report. Privacy International.

Privacy International (2019) Two states admit bulk interception practices: Why does it matter? Technical report. Privacy International.

Raleigh, Clionadh and Håvard Hegre (2009) Population size, concentration, and civil war. A geographically disaggregated analysis. *Political Geography* 28(4): 224–238.

Right2Know (2016) The surveillance state: Communications surveillance and privacy in South Africa. Technical report. The Media Policy and Democracy Project.

Roberts, T; A Mohamed Ali, M Farahat, R Oloyede and G Mutung'u (2021) Surveillance law in Africa: A review of six countries. Technical report. Brighton: Institute of Development Studies.

Roller, Lars-Hendrik and Leonard Waverman (2001) Telecommunications infrastructure and economic development: A simultaneous approach. *American Economic Review* 91(4): 909–923.

Ruttig, Thomas (2010) How tribal are the Taleban? Afghanistan's largest insurgent movement between its tribal roots and Islamist ideology. Technical report. Afghanistan Analysts Network Thematic Report 04/2010.

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

Saeed, Saim (2021) Taliban 2.0: Older, media-savvy and still duplicitous. *POLITICO* 20 August Accessed: 20.10.2021 (https://www.politico.eu/article/taliban-afghanistan-rebrand-social-media-twitter-international-recognition/).

Salverda, Nynke (2013) Blue helmets as targets: A quantitative analysis of rebel violence against peacekeepers, 1989-2003. *Journal of Peace Research* 50(6): 707 – 720.

Schubiger, Livia Isabella and Matthew Zelina (2017) Ideology in armed groups. *PS: Political Science & Politics* 50(4): 948–952.

Schutte, Sebastian and Karsten Donnay (2014) Matched wake analysis: Finding causal relationships in spatiotemporal event data. *Political Geography 41*: 1–10.

Schwartz, Joshua A; Matthew Fuhrmann and Michael C Horowitz (2022) Do armed drones counter terrorism, or are they counterproductive? Evidence from eighteen countries. *International Studies Quarterly* 66(3) sqac047.

Sediqi, Abdul Qadir and Rupam Jain (2019) Taliban fighters double as reporters to wage Afghan Digital War. *Reuters* 11 May Accessed: 20.10.2021 (https://www.reuters.com/article/us-afghanistan-taliban-media/taliban-fighters-double-as-reporters-to-wage-afghan-digital-war-idUSKCN1SH035).

Shapiro, Jacob N and David A Siegel (2015) Coordination and security: How mobile communications affect insurgency. *Journal of Peace Research* 52(3): 312–322.

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(2): 247–274.

Shaver, Andrew and Jacob N Shapiro (2021) The effect of civilian casualties on wartime informing: Evidence from the Iraq war. *Journal of Conflict Resolution* 65(7-8): 1337–1377.

Shaver, Andrew and Austin Wright (2016) Are modern insurgencies predictable? New evidence from Afghanistan and Iraq.

Shevory, Kristina (2016) Once a bright spot, Afghan telecoms face unsustainable losses. *The New York Times* 8 April (https://www.nytimes.com/2016/04/09/business/international/once-a-bright-spot-afghan-telecoms-face-unsustainable-losses.html).

Singer, J David (1988) Reconstructing the correlates of war dataset on material capabilities of states, 1816-1985. *International Interactions* 14(2): 115–132.

Soifer, Hillel (2008) State infrastructural power: Approaches to conceptualization and measurement. *Studies in Comparative International Development 43*: 231–251.

Soifer, Hillel David and Matthias vom Hau (2008) Unpacking the strength of the state: The utility of state infrastructural power. *Studies in Comparative International Development* 43(3-4): 219–230.

Staniland, Paul (2015) Militias, ideology, and the state. *Journal of Conflict Resolution* 59(5): 770–793.

Stanton, Jessica A (2013) Terrorism in the context of civil war. *The Journal of Politics* 75(4): 1009–1022.

START (2021) The Global Terrorism Database (GTD) Codebook. (https://www.start.umd.edu/gtd/downloads/Codebook.pdf).

Strick van Linschoten, Alex and Felix Kuehn (2018) *The Taliban Reader: War, Islam and Politics in their Own Words*. Oxford University Press.

Sundberg, Ralph and Erik Melander (2013) Introducing the UCDP Georeferenced Event Dataset. *Journal of Peace Research* 50(4): 523–532.

Telenor Group (2021a) Calling for a return to full mobile internet in Myanmar. Accessed: 23.01.2023 (https://www.telenor.com/media/newsroom/calling-for-a-return-to-full-mobile-internet-in-myanmar/).

Telenor Group (2021b) Continued presence in Myanmar not possible for Telenor. Accessed: 23.01.2023 (https://www.telenor.com/media/newsroom/continued-presence-in-myanmar-not-possible-for-telenor/).

Telenor Group (2021c) Telenor evaluates options in Myanmar. Accessed: 23.01.2023 (https://www.telenor.com/media/newsroom/telenor-evaluates-options-in-myanmar/).

Telenor Group (2021d) Telenor Myanmar pays annual licence fee under strong protest - calls for immediate opening of Data Network. Accessed: 23.01.2023 (https://www.telenor.com/media/newsroom/telenor-myanmar-pays-annual-licence-fee-under-strong-protest-calls-for-immediate-opening-of-data-network/).

Telenor Group (2021e) Update on the ongoing OECD complaint against Telenor on the sale of Telenor Myanmar (27 September 2021). Accessed: 23.01.2023 (https://www.telenor.com/media/newsroom/update-on-the-ongoing-oecd-complaint-against-telenor-on-the-sale-of-telenor-myanmar-27-september-2021/).

Telenor Group (2022) We cannot make our employees in Myanmar delete data and break the law. Accessed: 23.01.2023

(https://www.telenor.com/media/newsroom/announcement/we-cannot-make-our-employees-in-myanmar-delete-data-and-break-the-law-update-by-jorgen-c-arentz-rostrup-evp-and-head-of-telenor-asia/).

The Himalayan Times (2016) Arson attack on 6 Ncell towers by Chand-led Maoists. *The Himalayan Times* 11 June (https://thehimalayantimes.com/nepal/least-5-ncell-towers-put-fire-chand-led-maoists/).

The Times of India (2015) Maoists torch third mobile tower in Koraput in 10 days. *The Times of India* 22 December (https://timesofindia.indiatimes.com/city/bhubaneswar/maoists-torch-third-mobile-tower-in-koraput-in-10-days/articleshow/50276894.cms).

Themnér, Lotta and Peter Wallensteen (2014) Armed conflicts, 1946-2013. *Journal of Peace Research* 51(4): 541–554.

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

UCDP (no date) Government of United States of America - al-Qaida. Accessed: 28.04.2021 (https://ucdp.uu.se/statebased/878).

Unver, Hamid Akın (2018) Digital open source intelligence and international security: A primer. Technical report. Centre for Economics and Foreign Policy Studies.

Van Belle, Douglas A (1997) Press freedom and the democratic peace. *Journal of Peace Research* 34(4): 405–414.

Vogt, Manuel; Nils-Christian Bormann, Seraina Rüegger, Lars-Erik Cederman, Philipp Hunziker and Luc Girardin (2015) Integrating data on ethnicity, geography, and conflict: The Ethnic Power Relations data set family. *Journal of Conflict Resolution* 59(7): 1327–1342.

Vu, Khuong; Payam Hanafizadeh and Erik Bohlin (2020) ICT as a driver of economic growth: A survey of the literature and directions for future research. *Telecommunications Policy* 44(2): 101922.

Vu, Khuong M (2011) ICT as a source of economic growth in the information age: Empirical evidence from the 1996-2005 period. *Telecommunications Policy* 35(4): 357–372.

Walter, Barbara F. (2017) The new new civil wars. *Annual Review of Political Science* 20(1): 469 – 486.

Warren, Camber T (2014) Not by the sword alone: Soft power, mass media, and the production of state sovereignty. *International Organization* 68(1): 111 – 141.

Warren, T Camber (2015) Explosive connections? Mass media, social media, and the geography of collective violence in African states. *Journal of Peace Research* 52(3): 297–311.

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

Weidmann, Nils B and Espen Geelmuyden Rød (2019) *The Internet and Political Protest in Autocracies*. New York: Oxford University Press.

Wesal, Ajmal (2018) Taliban torch 2 telephone towers in Uruzgan. *Pajhwok Afghan News* 14 July (https://www.pajhwok.com/en/2018/07/14/taliban-torch-2-telephone-towers-uruzgan).

Williams, Daniel and Eric Guttschuss (2012) Spiraling violence: Boko Haram attacks and security force abuses in Nigeria. *Human Rights Watch* 11 October (https://www.hrw.org/report/2012/10/11/spiraling-violence/boko-haram-attacks-and-security-force-abuses-nigeria).

Wong, Belle JD (2023) Top social media statistics and trends of 2023. *Forbes* 18 May Accessed: 16.07.2023 (https://www.forbes.com/advisor/business/social-media-statistics/).

Wood, Elisabeth Jean (2006) Variation in sexual violence during war. *Politics & Society* 34(3): 307–342.

Wood, Reed M and Jakana L Thomas (2017) Women on the frontline: Rebel group ideology and women's participations in violent rebellion. *Journal of Peace Research* 54(1): 31–46.

Xu, Xu (2021) To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science* 65(2): 309–325.

Yanagizawa-Drott, David (2014) Propaganda and conflict: Evidence from the Rwandan Genocide. *The Quarterly Journal of Economics* 129(4): 1947 – 1994.

Yashar, Deborah J (2005) *Contesting Citizenship in Latin America: The Rise of Indigenous Movements and the Postliberal Challenge*. Cambridge Studies in Contentious Politics. Cambridge University Press.

Young, Joseph K. (2013) Repression, dissent, and the onset of civil war. *Political Research Quarterly* 66(3): 516–532.

Zeitzoff, Thomas (2017) How social media is changing conflict. *Journal of Conflict Resolution* 61(9): 1970–1991.

Zeitzoff, Thomas (2018) Does social media influence conflict? Evidence from the 2012 Gaza Conflict. *Journal of Conflict Resolution* 62(1): 29–63.

Zhou, Paul (2019) Why are governments around the world subsidizing 5G? *Light Reading* 23 September Accessed: 16.07.2023 (https://www.lightreading.com/partner-perspectives-(sponsored-content)/why-are-governments-around-the-world-subsidizing-5g/a/d-id/754298).