

# Contents

<i>Acknowledgments</i>	vii
<i>List of Figures</i>	ix
<i>List of Tables</i>	xi
1. Introduction	1
1.1 Argument	5
1.2 Evidence	9
1.3 Plan of the book	15
2. What are online controls, and how do they work?	18
2.1 Connecting to the Internet	18
2.2 Censorship	20
2.3 Monitoring content and people	34
3. Theory	40
3.1 The role of information in repression	41
3.2 The logic of online surveillance	46
3.3 The logic of online censorship	51
4. Online controls and repression in Syria	60
4.1 Information control for regime stability	60
4.2 Digital politics pre-conflict	62
4.3 2011 uprising and repression	64
4.4 Digital politics following the uprising	67
4.5 Studying repression in Syria: data and measurement	70
5. Nationwide shutdowns and government offensives	78
5.1 Understanding full shutdowns	81
5.2 Internet shutdowns and documented violence	87
5.3 Underreporting during shutdowns	94
6. Internet accessibility and targeted violence	98
6.1 When is online surveillance useful?	98
6.2 Regional Internet accessibility in Syria	100
6.3 Measuring the regime's violent strategy	102
6.4 Subnational evidence	105
7. Online controls and the protest-repression nexus in Iran	113
7.1 Elections and protest in 2009	114

7.2 Ramping up online controls after 2009	115
7.3 Protests and Internet shutdown, November 2019	120
8. Global evidence	130
8.1 How to measure Internet outages	131
8.2 Internet outages and political institutions	134
8.3 Internet outages and state repression	135
9. Conclusion	141
9.1 Summary of findings	141
9.2 The implications of tech-supported repression	143
9.3 Resistance to online repression	147
9.4 Beyond state control: the role of private companies	149
<i>Notes</i>	151
<i>Bibliography</i>	155
<i>Index</i>	177