CPH TECH POLICY BRIEF #8

MAY 2024

PUBLISHED BY THE QUEEN MARY'S CENTRE, COPENHAGEN CENTER FOR SOCIAL DATA SCIENCE & DEPARTMENT OF POLITICAL SCIENCE / UNIVERSITY OF COPENHAGEN

# REPRESSION IN THE DIGITAL AGE

BY ANITA GOHDES

This CPH Tech Policy Brief is based on the book "Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence", published by Anita Gohdes in 2023. The brief gives a short introduction to the topic and main argument of the book and presents select findings and implications on how Internet accessibility and state repression play out in authoritarian countries.

## OVERVIEW

Amidst evolving debates around the Internet's impact on politics, Internet penetration across the world has exploded. Although liberal democracies were early adopters, autocratic countries have been making strides in catching up. And while most countries have worked hard to expand Internet access, many have simultaneously developed technological tools to control the flow of information that comes with this access. Because the Internet has become such an essential part of our daily lives, its control has far reaching consequences, including on contentious politics. This book studies how information control has changed in the digital age, and how access to new digital technologies has transformed violent state repression, presenting evidence from Syria, Iran, and a global comparative analysis. The key finding is that digital surveillance and censorship take on a supportive role in states' repressive strategies, allowing them to more effectively repress citizen, both in war and peacetime. As digital communication becomes a bedrock of modern opposition and protest movements, understanding the role of technology in repression has become more important than ever.

## SURVEILLANCE AND CENSORSHIP IN THE DIGITAL AGE

The book argues that cyber controls present themselves as natural additions to governments' arsenal of repressive tactics. Cyber controls are defined as activities undertaken by or on behalf of state authorities with the aim of either monitoring, filtering, or blocking communication and information on the Internet. Cyber controls have changed the mechanisms of state access and control to information. The infrastructure of online surveillance and censorship has transformed traditional forms of gathering and controlling information for the purpose of raising the costs of collective mobilization. Overall the expectation is that online surveillance support the use of targeted violence, whereas restrictions of access to the Internet are likely to occur in the context of mass repression.

## REPRESSION TECHNOLOGY IN SYRIA

Syria was arguably the first country to employ a full arsenal of digital controls in conjunction with mass repression in the context of a large-scale civil conflict. In the early years of the conflict, it was frequently referred to as "the most socially mediated civil conflict in history"[1], with events painstakingly captured, documented, and communicated via the Internet. From the earliest days of the Syrian uprising in 2011, activists within and outside the country used countless social media accounts to inform each other about military operations and massacres and to help organize and coordinate.

The Assad regime has used an array of methods to spy on the country's population, such as the use of commercial spyware, DDoS attacks by the Syrian Electronic Army, and even detaining individuals in order to obtain Facebook and Twitter passwords. It has also fully or partially shut down Internet access on a frequent basis, thereby cutting millions of people's access to communication.

## DIGITAL INFRASTRUCTURE IN SYRIA AND IRAN

Syria and Iran both fall into the category of countries that exhibit high levels of centralization when it comes to their domestic Internet infrastructure. In 2012, Renesys estimated that 132 countries worldwide were at severe or significant risk of experiencing Internet shutdowns[2] due to the low diversity in their telecommunications sector. In both Syria and Iran the telecom sector is centralized in ways that puts the control of access to the Internet into the hands of a few decision-makers[2].

In 2011, the year of the civilian uprising in Syria and the implementation of its first nationwide shutdown, Syrian access to the Internet primarily depended on one provider, the state-owned Syrian Telecommunications Establishment (STE). In the same year, 71 countries were estimated to have fewer than ten service providers, including Iran. Iran's domestic Internet infrastructure has significantly developed over the past decade, yet despite these developments and the growing influence the country has achieved through network provision in the region, its access to the global Internet remains dependent on two entities that essentially serve as chokepoints to the digital outside world[3].

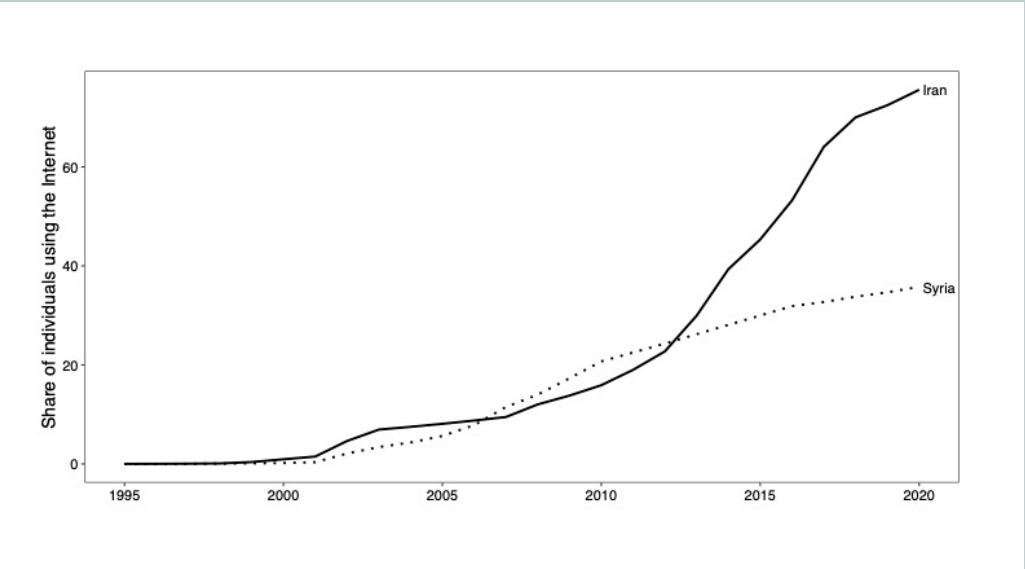
## RESEARCH DESIGN AND DATA

The book draws on evidence from large-scale quantitative analyses of violence perpetrated in the Syrian conflict, qualitative case evidence from internet shutdowns and protest crackdowns Iran, and presents a global comparative analysis of Internet outages and state repression. To study violence in Syria, an integrated database on state violence was built to cover the early years of the conflict (2011 to 2015). In Iran, the mass protests that spread across the country in November 2019 are studied in order to understand how Iranian security forces engaged in violent repression during the regime-ordered nationwide shutdown of the Internet. Insights from NGO and news reports, network measurement data on the Internet shutdown, and data on censorship circumvention are combined. Using global network measurement data, the book also presents a worldwide comparative analysis of the relationship between Internet outages and state repression.

## FINDINGS

- The results of the analysis of network outages and daily conflict fatalities in Syria suggests that the government implemented large-scale disruptions selectively and purposely in conjunction with concerted violent repressive offensives against the opposition.
- When and where the Syrian government provided Internet access and surveiled its population, repression tended to be highly targeted. Where the Internet was slowed or shut down, more violence was indiscriminate. Where the regime was able to rely on more traditional forms of intelligence (for example by having boots on the ground) digital surveillance played less of an important role.
- In Iran, the November 2019 Internet shutdown was accompanied by mass repression intended to cover up violence by security forces and motivate witnesses and bystanders to self-censor, even once the Internet was turned back on.
- At the global level, the results show that nationwide disruptions of the Internet are associated with higher levels of state-ordered repression.

**FIGURE 1** Development of Internet penetration in Syria and Iran




**Note:** Reproduction of Figure 1.2 in Gohdes (2023, page 11). Development of Internet penetration in Syria and Iran. Country-level Internet penetration data is collected by the International Telecommunication Union (ITU, 2022).

## IMPLICATIONS

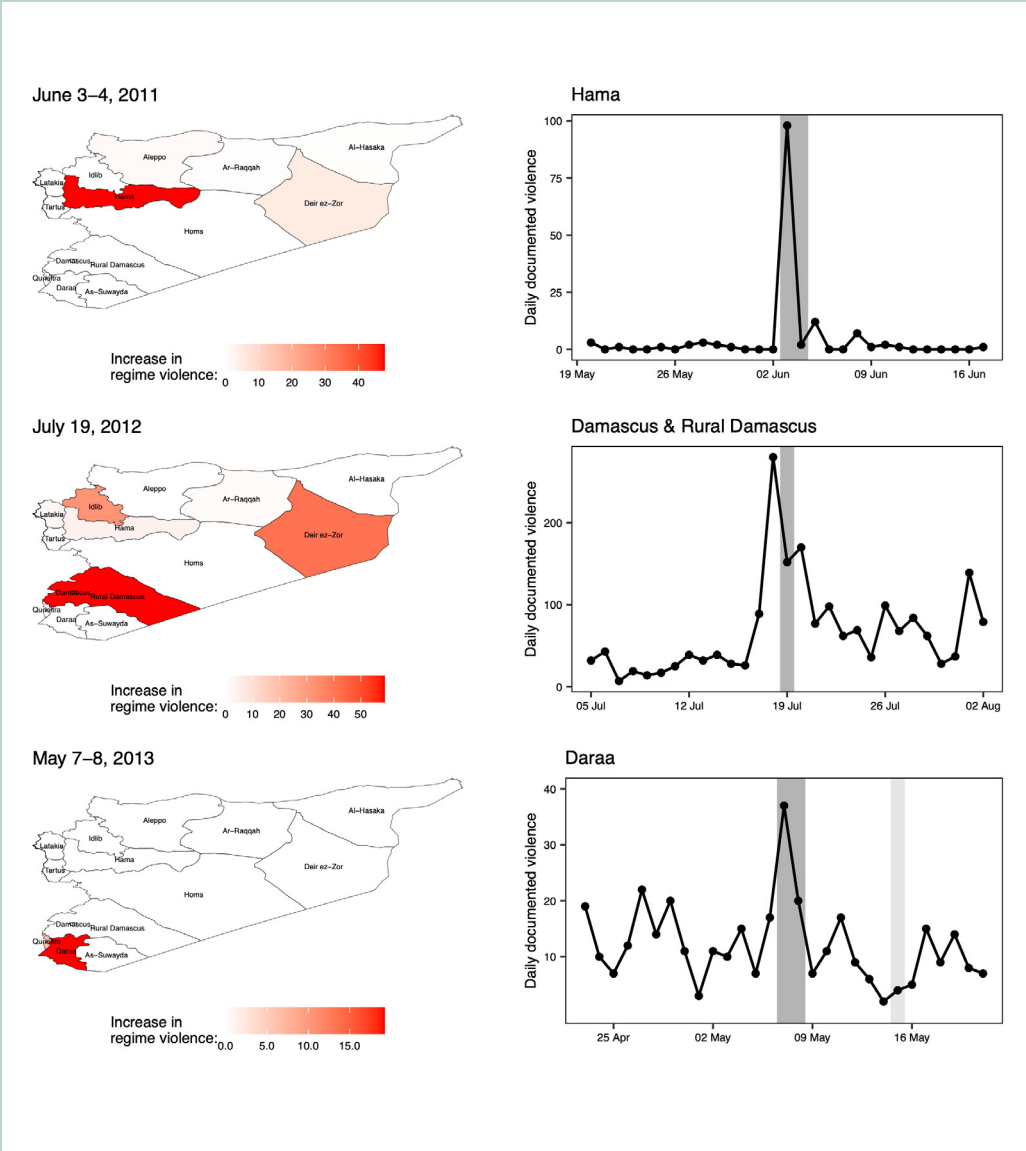
Taken together, the findings show that cyber controls are supporting security forces in their use of violent state repression: higher levels of Internet accessibility support more targeted violence, in particular in sectors of society that were previously shielded from state reach. Extreme forms of censorship or even shutdowns of the Internet occur in conjunction with larger and more indiscriminate repression.

Online surveillance has facilitated state access to previously hard to reach sectors of society as it bypasses the need for local in-person intelligence gathering that necessitates long-term investment in trustworthy personnel.

Online censorship has accelerated states' abilities to flexibly stifle or even shut down popular coordination and information exchange for short periods of time, thereby avoiding long-term information vacuums that could prove dangerous for regime stability

Shutting down access to the Internet can hamper the opposition's ability to coordinate, it can affect the functioning of their weapons systems, and it can help hide atrocities from the outside world. Whoever controls the Internet also has access to vast amounts of data, thereby providing an intelligence advantage.

**FIGURE 2** Difference in average number of killings by governorate during three of the seven nationwide Internet shutdowns




**Note:** Reproduction of Figure 5.1 in Gohdes (2023, page 89). Maps: Difference in average number of killings by governorate during three of the seven nationwide Internet shutdowns that occurred between 2011 and 2014. Difference is calculated by comparing average daily killings during the shutdown to average daily killings in the week preceding and the week following the shutdown. Only positive differences are reported to highlight core areas of fighting. Graphs: Daily numbers of documented regime killings for select governorates. Gray bars indicate days with nationwide Internet shutdowns.

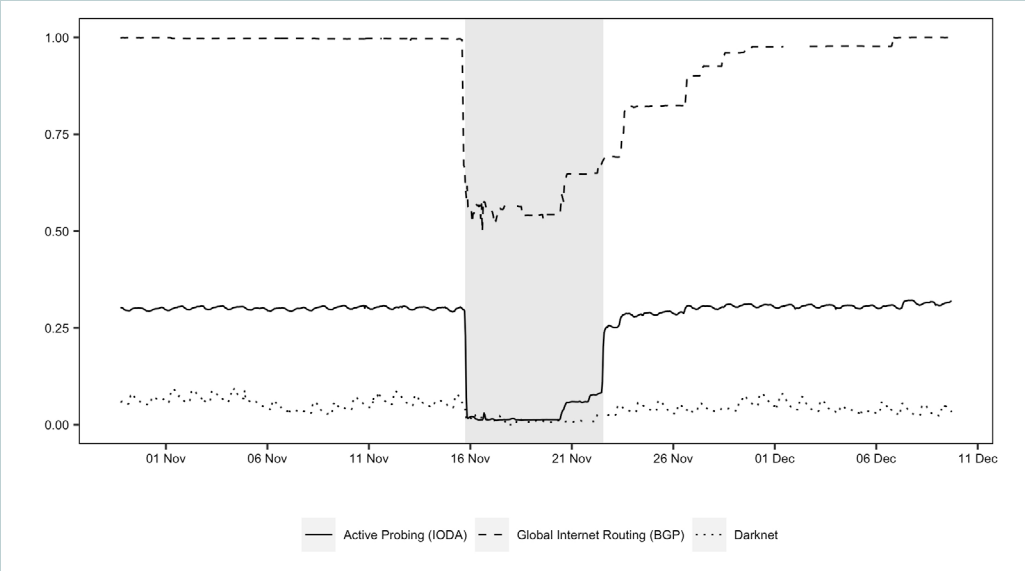
## DILEMMAS

- **Cutting social media takes a huge toll on civilians.** Civilians stuck in warzones are often desperate for information on where it is safe to go, whether their relatives and friends are safe, and where humanitarian aid is available. Rumors and disinformation can lead to actions that put civilians in direct harm. Social media is also an essential way for people in warzones to share their plight with the outside world. For many people outside of conflict zones, social media is often the first contact point to learn about a conflict. Conflict actors know this and can use propaganda to unsettle, confuse, and otherwise try and influence the outside world. But dynamics on social media are not always predictable, and to think that wartime information campaigns will always work is to overestimate the ability of people to be persuaded by what they see online.
- **The politics of digital infrastructure:** Internet access and control are not neutral. From Ethiopia, Yemen, to the Russian invasion of Ukraine: whoever controls the Internet has the ability to shut down access to it as part of military offensives. On numerous occasions when Russian forces invaded or occupied a territory within Ukraine, digital annexation occurred as an immediate consequence. How can digital annexation be prevented?

## POLICY RECOMMENDATIONS

- Digital infrastructure is highly political. The diversification of the Information and Telecommunications Sectors, in particular in authoritarian countries, can improve resilience against Internet shutdowns.
- Policy makers should pay special attention to the importance of export regulations of spyware and software used for content filtering.

**FIGURE 3** Normalized Internet traffic in Iran




**Note:** Reproduction of Figure 7.1 in Gohdes (2023, page 122). Normalized Internet traffic in Iran, November 15–25, 2019. Light gray area denotes the commonly understood nationwide Internet shutdown from the evening of November 16 until the early afternoon of November 23. Data source in graph: IODA.

## REFERENCES


1 Lynch, Marc, Deen Freelon, and Sean Aday. 2014. "Blogs and bullets III: Syria's social mediated war." United States Institute of Peace, Peaceworks 91(5).

2 Cowie, James. 2012. "Could an Internet blackout happen in your country?" Renesys Blog, November 30. https://bit.ly/3wD61bN .

3 Madory, Doug. 2019. "Historic Internet blackout in Iran." https://blogs.oracle.com/cloudsecurity/post/historic-internet-blackout-in-iran.

Gohdes, Anita R. 2023. Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence. Oxford University Press.