CHARLES UNIVERSITY
FACULTY OF SOCIAL SCIENCES
Institute of Communication Studies and Journalism

Master's Thesis

2024 **Hoi Ming Tsui**

CHARLES UNIVERSITY
FACULTY OF SOCIAL SCIENCES
Institute of Communication Studies and Journalism

Fourth Estate in the Dark: Examining the Tactics Employed by Journalists During Internet Shutdown

Master's Thesis

Author of the Thesis: Hoi Ming Tsui, BA
Study programme: Erasmus Mundus Journalism
Supervisor: Mgr. František Géla

Year of the defence: 2024

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.
4. During the preparation of this thesis, the author used GoodTape in order to transcribe and translate. After using this tool/service, the author reviewed and edited the content as necessary and takes full responsibility for the content of the publication.

In Prague on **20 July 2024**

Hoi Ming Tsui

References

TSUI, Hoi Ming. *Fourth Estate in the Dark: Examining the Tactics Employed by Journalists During Internet Shutdown.* Praha, 2024. 73 s. Master's thesis (MA). Charles University, Faculty of Social Sciences, Institute of Communication Studies and Journalism. Supervisor Mgr. František Géla.

Length of the Thesis: 103, 812 characters with spaces

Abstract

Internet shutdowns have increasingly become a tactic employed by governments worldwide to restrict press freedom. This research aims to investigate potential and existing efficient methods for maintaining journalism during internet shutdowns, based on in-depth interviews with three experts and eight journalists from regions affected by shutdowns. The results show that common challenges journalists face during shutdowns include difficulties in communicating with different parties, and increased government oppression. The findings highlight several technological solutions, such as the use of different tools, as well as the potential of satellite technology as an alternative source of internet. Regarding non-technological circumvention, journalists emphasized the importance of maintaining a network within both locally and internationally, as well as setting up contingency plans in advance. Given the difficulties in circumventing a full shutdown, journalists stressed the importance of recording and archiving news events. There is no one-size-fits-all solution to shutdowns; effective strategies depend on various factors such as the scale and local laws regarding certain technologies. The international communities are encouraged to engage with locals, and to continue developing circumvention tools to address the ever-changing political and technical landscape. Methods for categorizing internet shutdowns should also be reviewed to more effectively identify solutions.

Abstrakt

Vypínání internetu se stále častěji stává taktikou, kterou vlády po celém světě používají k omezování svobody tisku. Cílem tohoto výzkumu je na základě hloubkových rozhovorů se třemi odborníky a osmi novináři z regionů postižených výpadky internetu, prozkoumat možné a existující účinné metody pro zachování chodu kvalitní žurnalistiky během výpadků. Výsledky ukazují, že mezi běžné problémy, kterým novináři během výpadků čelí, patří obtíže při komunikaci s různými stranami a zvýšený útlak ze strany vlády. Zjištění poukazují na několik technologických řešení, jako je používání různých nástrojů, a také na potenciál satelitní technologie jako alternativního zdroje internetu. Co se týče netechnologického obcházení, novináři zdůraznili důležitost udržování sítě kontaktů lokálních i mezinárodních, stejně jako vytváření krizových plánů v předstihu. Vzhledem k obtížím při obcházení úplného vypnutí internetu, novináři zdůraznili význam nahrávání a archivace zpravodajskýchp událostí. Neexistuje žádné univerzální řešení vypnutí; účinné strategie závisí na různých faktorech, jako je rozsah a místní zákony týkající se určitých technologií. Mezinárodní komunity se vyzývají, aby spolupracovaly s místními obyvateli a pokračovaly

ve vývoji nástrojů pro obcházení, které by reagovaly na neustále se měnící politické a technické podmínky. Měly by se také přezkoumat metody kategorizace vypínání internetu, aby bylo možné účinněji určit řešení.

Keywords

Internet shutdown, press freedom, rights to know, digital rights, internet freedom, killswitch, freedom of expression, internet, internet access

Klíčová slova

vypnutí internetu, svoboda tisku, právo na informace, digitální práva, svoboda internetu, killswitch, svoboda projevu, internet, přístup k internetu

Title

Fourth Estate in the Dark: Examining the Tactics Employed by Journalists During Internet Shutdown

Název práce

Čtvrtá velmoc v temnotě: Analýza novinářské praxe při výpadku internetu

Acknowledgement

First of all, I would like to express my gratitude to all the journalists who participated in this research, sharing sensitive information based on trust to help achieve a freer internet and greater press freedom. Secondly, I want to thank and salute all journalists working under internet shutdowns for their persistence in giving the underrepresented a voice even during such a tough situation. I, and the rest of the world, know about what is happening in those countries because they risk their freedom or even lives to report the truth. Thirdly, I would like to applaud all technologists, human rights advocates, and digital rights defenders, including the three experts interviewed, who have been fighting against internet shutdowns and dedicating their time to safeguarding the right to know and promoting an open internet.

I would also like to thank my consultant, PhDr. David Erkomaishvili, Ph.D., for his voluntarily support and constructive feedback.

Lastly, I pay tribute to Aaron Swartz for everything he had done and his inspirational quote: “There is no justice in following unjust laws. It’s time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture. We need to take information, wherever it is stored, make our copies and share them with the world.”

Institute of Communication Studies and Journalism FSV UK
Research proposal for Erasmus Mundus Journalism Diploma Thesis

THIS PART TO BE FILLED BY STUDENT:

Student's surname and given name:
Tsui Hoi Ming

Start of studies for EMJ (in Aarhus)
Sept 2022

Your faculty e-mail:
64722150@fsv.cuni.cz

Study program/form of study:
Erasmus Mundus Journalism

Registry stamp: / Razítko podatelny:

Univerzita Karlova
Fakulta sociálních věd
Došlo dne: 14 -11- 2023 -1-
Čj: 443 Přiloh:
Přidělено:

Thesis title in English:
Fourth Estate in the Dark: Examining the Tactics Employed by Journalists during Internet Shutdown

Expected date of submission (semester, academic year)
(Thesis must be submitted according to the Academic Calendar.)
Summer semester of 2023/2024

Main research question (max. 250 characters)**:**

1. How do journalists cope with internet shutdown?
    a. How effective are the methods in the finding? Are there any limitations and shortcomings?
    b. How can the above methods be further utilized for journalism purposes during a shutdown?

Current state of research on the topic (max. 1800 characters)**:**

Literature review and interview conducted for research purposes:
In today's digital-driven world, authoritarian governments often impose internet shutdowns to restrict the flow of information, particularly during social events like protests or uprisings (AccessNow, 2020). Consequently, journalists face difficulties in obtaining current event information and publishing news.

Governments can implement internet shutdowns in various ways, resulting in different levels of difficulty in bypassing them (Deibert et al., 2008). Internet shutdowns tend to worsen human rights abuses and interfere with democratic processes (Selnes, 2021). To address this, digital rights advocates and technology experts worldwide have developed communication channels such as mesh networks, which do not rely on the Internet to facilitate communication (Albrecht et al.,2021). These networks create a functioning system without internet access. Another example is satellite technology, where media can broadcast packets of content, including news videos, without relying on the Internet (Allagui & Kuebler, 2011). This is particularly useful in cases where public broadcasters are typically biased.

However, based on the initial interview with digital rights advocates, hacktivists, and founders of communication channels, it is evident that the user data is unobtainable and unclear. Additionally, there appears to be a gap between existing tools or workarounds and actual use cases. On the other hand,

some journalists rely on government-provided internet centers or traditional SMS communication, while others simply reduce their communication and reporting activities.

Expected theoretical framework (max. 1800 characters)**:**

- Technological Determinism (McLuhan, 1994): It suggests that technological advancements shape how societies think, behave, and organize. This theory explores the influence of technology on human society, emphasizing its role as a primary driver of social progress.
- Liberal Theory (Ash, 2016; Mill, 2011) - Liberal theory is a political and social philosophy emphasizing individual freedom, rights, and equal opportunities. It advocates for limited government intervention in people's lives and promotes democratic principles, such as freedom of speech, religion, and assembly.
- Diffusion of innovations theory (Rogers, 2003): The Diffusion of Innovations theory, developed by Everett Rogers, explores how new ideas or innovations spread in a society. It categorizes adopters into groups (innovators, early adopters, early majority, late majority, and laggards) based on their readiness to accept innovations. Understanding these dynamics is crucial for predicting and facilitating the adoption of new technologies or practices.
- Access theory (Burnett et al., 2008; Deibert et al., 2008): it focuses on ensuring equitable access to information resources, knowledge, and opportunities for all individuals, regardless of their socioeconomic status, geographic location, or other factors that might create barriers to access.

Expected methodology, and methods for data gathering and analysis (max. 1800 characters)**:**

Qualitative research method: in-depth interviews:
For the purpose of this research, a qualitative research method will be used. This will involve conducting sentiment analysis of comments, as well as sampling technology experts and journalists who have experience working under internet shutdowns. The goal is to identify current practices and explore potential options for media workers in areas affected by internet outages.

For interviews of journalists, semi-structured in-depth interviews with a set of open-ended questions will be used to look into experience in working in journalism under internet shutdown. Follow-up questions will make it possible to get a greater inside into their experiences and thoughts given the different political contexts in different regions. Meanwhile, for the interviews of experts, in-depth, descriptive questions will be used, depending on the interviewees' expertise or their respective research focus.

Expected research design (data to be analyzed, for example, the titles of analyzed newspapers and selected time period):

The data to be analyzed will consist of responses from interviews conducted with five technology experts specializing in internet freedom and press freedom. Purposive sampling was used to select these experts. Additionally, responses from 5 journalists who have experience working under internet shutdowns will be included in the analysis. Snowball sampling was used to select these journalists.

For the selection of experts, the purposive method will be used. They will be selected based on their expertise and the projects they have founded.

For the selection of journalists, the snowball sampling method will be used. I will ask people in my professional network and existing interviewees to refer more interviewees to me. This method is appropriate as media outlets are often cautious and need to protect the identity of journalists working in states or countries that limit the flow of information, which tend to be authoritarian countries.Therefore, personal referral will be needed.

Expected thesis structure (chapters and subchapters with brief description of their content):

1. Introduction
2. Internet shutdown
    - What is internet shutdown
    - Common ways for government to shutdown internet
    - Brief situation and data about current internet shutdown
3. Literature review
4. Theoretical framework
5. Research question
6. Research Design And Methods
7. Results
    - Existing technology and recommendation by experts
    - Current practice of how journalists communicate and publish during internet shutdown
    - Efficiency of the current practices
    - Use case studies
8. Discussion / conclusion
9. Limitation

Basic literature list (at least 5 most important works related to the topic and the method(s) of analysis; all works should be briefly characterized on 2-5 lines):

- AccessNow. (2020, February). Targeted, cut off, and left in the dark. https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf
  (A conclusion and global overview of internet shutdown cases and development)

- Albrecht, M. R., Blasco, J., Jensen, R. B., & Mareková, L. (2021). Mesh Messaging in Large-Scale Protests: Breaking Bridgefy. In K. G. Paterson (Ed.), Topics in Cryptology – CT-RSA 2021 (Vol. 12704, pp. 375–398). Springer International Publishing. https://doi.org/10.1007/978-3-030-75539-3_16
  (Literature about the theory and usage of mesh network in protests, which experts commonly recommend for the purpose of communication during internet shutdown.)

- Allagui, I., & Kuebler, J. (2011). The Arab Spring and the Role of ICTs| Introduction. International Journal Of Communication, 5, 8. Retrieved from https://ijoc.org/index.php/ijoc/article/view/1392/616
  (Literature about internet shutdown during Arab Spring, and the technology workaround that was suggested and adapted at the time.)

- Ash, T. G. (2016). Free speech: Ten Principles for a Connected World. Yale University Press.
  (Literature about Liberal theory, explores the relationship between press freedom and internet access, at the same time advocating for limited government intervention in freedom of speech.)

- Deterding, N. M., & Waters, M. C. (2021). Flexible Coding of In-depth Interviews: A Twenty-first-century Approach. *Sociological Methods & Research*, *50*(2), 708-739. https://doi.org/10.1177/0049124118799377
  (Literature about my research method, especially in-depth interview.)

- Knott, E., Rao, A.H., Summers, K. *et al.* Interviews in the social sciences. *Nat Rev Methods Primers* **2**, 73 (2022). https://doi.org/10.1038/s43586-022-00150-6
  (Describing different sampling methods for qualitative research)

- Mahler, A., & Rogers, E. M. (1999). The diffusion of interactive communication innovations and the critical mass: The adoption of telecommunications services by German banks. Telecommunications Policy, 23(10–11), 719–740. https://doi.org/10.1016/S0308-5961(99)00052-X
  (Full explanation of Diffusion of innovations theory, explaining how technology gets adapted into a society)

- McLuhan, M. (1994). Understanding media: The Extensions of Man. MIT Press.
  (Literature about Technological Determinism illustrates how media affect the development of society and how technology affects democracy and civil rights.)

- Mill, J. (2011). Of the limits to the authority of society over the individual. In On Liberty (Cambridge Library Collection - Philosophy, pp. 134-167). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139149785
  (Talks about liberty theory and freedom of the press.)

- Selnes, F. N. (2021). Internet restrictions in Uganda: Examining their impact on journalism. Information, Communication & Society, 24(3), 490–506. https://doi.org/10.1080/1369118X.2020.1859580
  (Literature about internet shutdown and journalistic work, as well as press freedom.)

Related theses and dissertations (list of B.A., M.A. and Ph.D. theses defended at Charles University or other academic institutions in the last five years):

Date / Signature of the student:

[redacted]

.....

THIS PART TO BE FILLED BY THE ACADEMIC SUPERVISOR:
I confirm that I have consulted this research proposal with the author and that the proposal is related to my field of expertise at the Faculty of Social Sciences. **I agree to be the Thesis supervisor.** [redacted]
Surname and name of the supervisor **Date / Signature of the supervisor**
Further recommendations related to the topic, structure and methods for analysis:
Further recommendations of literature related to the topic:

The research proposal has to be printed, signed and submitted to the FSV UK registry office (podatelna) in two copies, **by November 15**, addressed to the Program Coordinator. Accepted research proposals have to be picked up at the Program Coordinator's Office, Sandra Lábová. The accepted research proposal needs to be included in the hard copy version of the submitted thesis.

RESEARCH PROPOSALS NEED TO BE APPROVED BY THE HEAD OF ERASMUS MUNDUS JOURNALISM PROGRAM.

Table of Contents

Introduction 10

1. Theoretical perspectives 12

2. What is internet Shutdown 13

2.1 How the Internet Works 13

2.2 Defining Internet Shutdown 14

2.3 How to Shut Down the Internet 15

3. Literature Review 16

3.1 Pattern Of internet Shutdown 16

3.2 Triggers of Internet Shutdown 17

3.3 Effect of Internet Shutdown 18

3.4 Shutdown Circumvention 19

3.4.1 Non-technological fix 19

3.4.2 Technological fix 20

3.4.3 Seeking External Help From Human Rights Organisations 21

3.4.4 Constrain of Combatting internet Shutdown 22

3.4.5 Literature Review Conclusion 22

4. Methodology 23

4.1 Data collection and sampling 23

4.1.1 Interview with experts 24

4.1.2 Interview with Journalists 25

4.2 Analysis 26

5. Findings 27

5.1 Main Challenges Journalists Face During Internet Shutdown 27

5.1.1 Communication Challenges During Internet Shutdowns 27

5.1.2 Difficulties in Conducting Research and Fact-checking Due to Media Blackout 28

5.1.2 Lack Of Knowledge Regarding internet Shutdown 29

5.1.3 Increase Oppressiveness Targeting Media From Governments 30
5.2 Technological Solution for Journalists 31
5.2.1 Use of Virtual Private Network (VPN) 31
5.2.2 Use of Offline Instant Messenger Tools 33
5.2.3 Readapting Legacy Communication System 34
5.2.4 Satellite Technology as an Alternative Source of Internet 35
5.2.5 Building an Offline News Archive 37
5.3 Non-technological Solution for Journalists 37
5.3.1 The Importance of Building a Network, Both within the Community and Internationally 37
5.3.2 Importance of Setting Up Contingency Plans in Advance 38
5.3.3 Working With And Building Connections With Diaspora Communities 40
5.4 Focusing on Recording and Archiving News Events Due to Lack of Solutions for Full Blackouts 40
5.5 Leveraging Solutions in the Face of Varied Threats and Contexts 42
5.6 Suggestions for human rights organisations and technological communities 44
5.6.1 Providing Training For Local Journalists and Civil Society 44
5.6.2 Continuous Development and Updating of Circumvention Tools 46
5.6.3 The Importance of Local Engagement and Avoiding a Top-Down Approach 47
5.6.4 Providing Financial Support for Local Journalists in Shutdown Areas 48
5.6.5 Reviewing Methods for Categorising Internet Shutdowns 49
5.6 Constraints in Circumventing internet Shutdowns 50
5.6.1 Difficulties in Developing Circumvention Tools 50
5.6.2 The High Financial Cost of Combatting Shutdowns 51
6. Limitation 51
Conclusion and Discussion 52
Summary 55
List of References 57

Introduction

Internet shutdowns have increasingly become a popular tactic employed by governments worldwide to restrict press freedom and citizens' right to information (Feldstein, 2021; Satriawan et al., 2023), since Egypt's then-president Hosni Mubarak took the country offline for five days during the Arab Spring on January 27, 2011 (Arthur, 2011). This event opened Pandora's box of network interference incidents worldwide (Bischof et al., 2023).

The internet is often perceived as a tool for information sharing that transcends traditional media boundaries (Fuchs, 2007). As internet usage grows alongside the rise of social media, citizens worldwide have become better informed, and the threshold for bottom-up information sharing, which eventually affects public views and governance, has been lowered (Feldstein, 2021; Rydzak et al., 2020; Satriawan et al., 2023). For example, internet access enabling whistleblowers or independent journalists to expose public figures' scandals and address electoral violence while dodging increasing censorship in mainstream media. This improves citizens' knowledge about their choices (Garbe, 2023; Grinko et al., 2022; Richey & Taylor, 2018) and mobilises uprisings from grassroots movements, as internet access provides an easy way for protesters to communicate and organise without a leader (Chari, 2024; Feldstein, 2021; Garbe, 2023; Satriawan et al., 2023). In short, widespread internet accessibility has ever since changed the media landscape, breaking down various barriers to information access, ranging from geographical barriers, allowing global news access, to language barriers, enabling information translation into other languages (Chari, 2024).

At the same time, governments worldwide have noticed the internet's power and have begun to employ a wide variety of methods to deploy internet restrictions. They justify these actions as necessary to prevent terrorism and attacks, and protect national security (Ayalew, 2019; Ryng et al., 2022; Selnes, 2020). On the other hand, citizens and international communities criticise these shutdowns as a means for authorities to suppress citizens' right to know and control narratives (Access Now, 2024; Ryng et al., 2022). The Committee to Protect Journalists (CPJ) (2021) stated, "internet shutdowns have serious consequences for press freedom and leave journalists struggling to do their job effectively."

In recent years, an increasing amount of literature and research has been dedicated to the topics of internet censorship, surveillance, and shutdowns. Various international non-profit

organisations focusing on digital rights, press freedom, and technology have been working to combat internet shutdowns through advocacy and developing tools to be used during shutdowns (Access Now, 2024), trying to help maintain the flow of information and protect human rights.

This research paper examines how journalists can cope with internet shutdowns to minimise the damage to their work and sustain journalism in affected regions, addressing the following research questions:

RQ1: How do journalists currently cope with internet shutdowns?
RQ2: What are the best ways for journalists to cope with internet shutdowns to sustain journalistic work?

To answer the questions, this thesis will first provide an overview of the existing literature on internet shutdowns, examining what scholars have researched and discovered on the topic. It will then present the theoretical perspective of freedom of expression for the information society, discussing how modern journalism has evolved due to the rise of the internet and how authorities attempt to restrict freedom of expression through technology. Following this, the methodology will be outlined, detailing how semi-structured interviews with both experts and journalists were thematically coded and analysed. Finally, the findings will be presented, followed by the conclusion, discussion, and limitations of this research.

1. Theoretical perspectives

The theoretical framework of this research is drawn from the theory of freedom of expression for the information society.

In the 1960s, the development of radio and television broadcast technologies sparked a digital revolution that converted technology from analogue format to digital format (Balkin, 2003). Scholars and politicians began to discuss freedom of speech in a new light. Free speech advocate, Alexander Meiklejohn (1965), emphasised the importance of free speech in democracy, stating that political systems should ensure that everything worth saying is said, but not necessarily that everyone should speak. Since then, this has become the generally accepted scope of free speech while democratic deliberation has been a focus of freedom of speech.

However, Balkin (2004) argues that the "digital revolution" with the rise of the internet has altered the social conditions of speech as it drastically lowers the costs of distributing information and makes broadcasting and publishing individuals' views cheaper and more accessible. This ease of information dissemination enables content to cross cultural and geographical borders, allowing citizens to innovate with and build upon existing information. .

Therefore, in the digital age, distribution and innovation go hand in hand, and freedom of speech should focus on individual autonomy and collective self-governance (Balkin, 2004), rather than focusing on restricting and preventing media concentration like in the past. On top of receiving news passively, modern journalism focus includes the active participation of citizens and independent journalists who can deliver news via social platforms such as Facebook or Twitter (now X). Media can obtain quotes and information from other sources, such as private communication channels of politicians, and Telegram groups organised by civil society, using them as launching pads for commentary. In this dynamic, listeners, like news audiences, will in turn become speakers themselves. Ultimately, in the digital age, a "democratic culture is a culture in which individuals have a fair opportunity to participate in the forms of meaning-making that constitute them as individuals" (p.3).

Under this premise, Balkin (2004) predicted that the second major battleground over freedom of speech would be telecommunications policy. He described that "technologies of distribution are the 'pipes' through which content travels" (p.17) argued that digital

technologies could introduce new methods of control, raising the critical question of "who will control these ‘pipes’." Entities who control these "pipes" would govern key communications networks, making them not freely accessible to all, and thus could restrict access to information and harm freedom of expression. He emphasised that broadcasters, cable companies, or satellite companies, which are subject to structural public-interest regulation, could be the possible controller of the “pipes” and wield significant control over these networks. He states, "freedom of speech will depend on the design of the technological infrastructure that supports the system of free expression and secures widespread democratic participation" (p. 5).

This prediction has been validated with the increasing case of internet shutdown, where “pipes” like ISPs control access to the internet, undermining free expression and the modern journalism model, with the order coming from the authorities, like the “owners” Balkin describes. Journalism is the foundation of free speech, as media serves as a vehicle for delivering the "raw material" of public opinion and democracy, thus enabling citizens to exercise their rights and responsibilities in a democratic society (Merrill, 1994). Therefore, this research aims to investigate not only technological methods but also other approaches for circumventing repressive regimes' restrictions on information flow and press freedom through internet shutdowns.

2. What is internet Shutdown

2.1 How the Internet Works

According to the Cambridge English Dictionary, the internet is defined as a “large system of connected computers around the world that allows people to share information and communicate with each other” (Cambridge University Press, n.d.). In this context, computers encompass not only desktop computers, but also various interconnected devices such as routers and servers managed by internet Service Providers (ISPs) like T-Mobiles or Vodafone, and backbone networks (Shuler, 2002). Each device connected to the internet is assigned a unique identifier called an IP address, which functions like the address of a house, enabling devices to locate each other and exchange data (Malan, 2017). An IP address typically appears as a series of characters, such as “142.250.1.1”. To make the experience of using the internet more user-friendly, DNS (Domain Name System) is developed to translate IP addresses into human-readable domain names (Comer, 2018). As Cloudflare explains, the

Domain Name System (DNS) serves as the internet's phonebook. For instance, the domain name google.com corresponds to the IP address 142.251.37.110[1], referring to the same destination by different names (Cloudfare, n.d.). In most countries, ISPs, organisations, or public DNS providers like Google DNS and Cloudflare DNS manage their own DNS servers, which vary in speed, privacy level, supported protocols, and other characteristics (Comer, 2018).

To facilitate communication and data exchange between devices, computer scientists have developed standardised "protocols" (Comer, 2018). These protocols define standardised methods for performing actions and formatting data to enable devices to communicate and comprehend each other's signals (Comer, 2018; Malan, 2017). Different protocols are tailored for different stages of data transmission. For example, Border Gateway Protocol (BGP) is a set of rules that determine the best network routes for data transmission on the internet (O'Neill et al., 1998); User Datagram Protocol (UDP) protocol is used specifically for streaming videos (O'Neill et al., 1998), and Hypertext Transfer Protocol (HTTP) is employed for formatting data for websites and applications (O'Neill et al., 1998).

While many people believe the internet is free, its operation involves multiple hierarchical physical infrastructures. These include undersea cables and fibre optics that carry data across continents and regions at high speeds, and cell towers that transmit and receive radio signals to and from mobile devices within the cellular network (Mare, 2020; Truscello, 2023). Additionally, the internet relies on multiple stakeholders such as DNS server operators, governments, and regulatory authorities, who manage the licensing of operators (Mare, 2020; Truscello, 2023). For individuals to access the internet, they must purchase services from internet Service Providers (ISPs), who allocate and manage bandwidth among customers and oversee the physical and virtual network infrastructure, including routers, switches, and cables (Foros & Hansen, 2001).

2.2 Defining Internet Shutdown

As there is increasing reporting and research about the topic, there are many different terms to describe an "internet shutdown", such as "network disruptions", "kill switches", and "information blackouts" (Bhatia et al., 2023). Ben Wagner (2018) pointed out that

[1] This is as of 23 June 2024, as large services like Google often have multiple IP addresses associated with their domain to handle traffic efficiently.

internet shutdowns differ from other forms of internet censorship as shutdowns “block all content and do not attempt to discriminate what kind of content they block, whereas internet censorship targets specific items or types of content” (p. 3921).

Different scholars and non-profit organisations have varying definitions of internet shutdowns. Some, like Access Now (2019), define it as “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information” (Taye & Access Now, 2019, p.2). This definition includes the blocking of major internet platforms such as Facebook or YouTube.

This paper adopts Access Now's definition to examine solutions and circumventions applicable to a wider variety of internet shutdown cases.

2.3 How to Shut Down the Internet

Technically, at its core, shutting down the internet means disrupting the flow of data from sender to receiver. With the various hierarchical physical infrastructures, stakeholders and regulatory authorities, it means that there are numerous point of penetration where internet shutdowns can be imposed, with different approaches, employing different legal means, and at different scales (Mare, 2020; Truscello, 2023).

For example, routing manipulation is one approach at the network level. It involves altering network routing to interrupt data traffic to other infrastructures (Björksten, 2022). During the Syrian civil war in 2012, the government withdrew BGP routes, effectively disconnecting Syria from the global internet (Shachtman, 2012). Another method is DNS-level interference, where authorities manipulate domain name servers or DNS traffic to redirect users to incorrect servers, preventing access to the correct domain name or IP address (Björksten, 2022).

Alternatively, at the infrastructure level, a fundamental infrastructure shutdown can occur through physical damage to communications infrastructure, such as turning off the power grid or destroying cell towers (Björksten, 2022). An example of this is Venezuela in 2019, where the government shut down the power grids during protests to cut off citizens’ access to the internet (Jones, 2019).

Another common method is throttling, where authorities artificially restrict the flow of data through a communications network, making it too slow to function effectively without stopping it completely (Björksten, 2022). These examples illustrate some of the current methods authorities worldwide use to shut down the internet, among many other possible approaches. Moreover, Access Now categorises internet shutdowns into different types: full network shutdowns, bandwidth throttling, and service-based blocking for two-way communication platforms. They also assess whether mobile and/or broadband networks are affected (Björksten, 2022).

On the other hand, legally, different governments have different laws that theoretically permit or grant authorities the right to shut down the internet (Madenga, 2021). Instead of having definitive laws to enforce internet shutdowns directly, many of these laws are often vague and lack clear guidelines on when and how to impose or lift shutdowns (Moinuddin, 2021). For instance, in Cameroon, authorities have used anti-terror and cybercrime laws to suppress the media. The vague terminology used in these laws, such as "conflict with the principles of public policy" and "attempt to undermine state security", leaves it open to interpretation by authorities to justify an internet shutdown (Ngangum, 2023). Moreover, Anti-Terrorism and Anti-Pornography related laws are commonly used justifications for internet shutdowns worldwide (Selnes, 2021).

3. Literature Review

3.1 Pattern Of internet Shutdown

Numerous literature and organisations have analysed the trend of internet shutdowns, all concluding that they are becoming increasingly common worldwide (Marchant, 2020; Ngangum, 2023). In 2023, there were at least 283 shutdowns in 39 countries documented, breaking the record of shutdown incidents in a single year (Rosson et al., 2024). In some countries, the duration of a shutdown is yearlong. For example, the Ethiopian government has endured over a two-and-a-half-year long of complete communications blackout in Tigray (Rosson et al., 2023), and in Myanmar, citizens had been in the dark for more than 500 days by March 2023 (Rosson et al., 2023). Meanwhile, India remains the country most often pointed to for its extreme approach to frequency (Feldstein, 2021; Marchant, 2020; Moinuddin, 2021; Ngangum, 2023). The geographic scope of shutdowns had also widened,

with only 30.4% of all shutdowns on the smallest scale[2] in 2023, compared to 46.8% of all shutdowns on this scale in 2022 (Rosson et al., 2024).

Internet shutdowns tend to occur in less developed, more authoritarian countries (Moinuddin, 2021; Rydzak et al., 2020). Scholars have established a causal relationship between authoritarianism, non-representative political institutions, military control of the government and media, and a higher likelihood of state ownership of the ISP space, which in turn increases the probability of shutdowns (Feldstein, 2021; Moinuddin, 2021). However, it has also been observed that several democracies and hybrid regimes, such as India, Pakistan, and Algeria, also resort to internet shutdowns (Feldstein, 2021; Truscello, 2023). Additionally, studies have found a correlation between a leader's longevity in power and the likelihood of implementing shutdowns (Feldstein, 2021; Rydzak et al., 2020). As of early 2019, among the 14 longest-serving leaders in Africa, only three had not ordered a shutdown during their tenure (Feldstein, 2021). This supports the observation that internet shutdowns are used as a means to maintain power by quelling uprisings or disrupting elections.

3.2 Triggers of Internet Shutdown

Among all the causes, elections, coups, and protests are significantly more likely to trigger internet shutdowns on days of events (Bischof et al., 2023; Feldstein, 2021; Madenga, 2021; Moinuddin, 2021; Satriawan et al., 2023; Selnes, 2021; Shah, 2021; Truscello, 2023; Wagner, 2018), as internet shutdowns are often used as a tool to suppress freedom of expression and prevent people from voicing their views (Moinuddin, 2021). In countries that lack sophisticated means to counter mass protests, this practice is more common (Feldstein, 2021). Authoritarian states typically use internet shutdowns to hinder protestors and civil society from mobilising movements. On some occasions, states would justify a shutdown by protecting public security and controlling the spread of misinformation, and this justification has also been used frequently during elections and conflicts (Marchant, 2020; Moinuddin, 2021; Shah, 2021). For example, in Benin, the government shut down the internet after the government's official Twitter account warned about the problems of misinformation on social media during the elections in 2019 (Marchant, 2020). However, this justification was also seen as a resort to prevent journalists or citizens from documenting state violence (Bhatia et al., 2023; Chari, 2024).

[2] According to Access Now's (2024) definition, the smallest scale of shutdowns mean a shutdown only affecting one city, county, or village (Rosson et al., 2024, p.8).

Sometimes, non-political factors can trigger a shutdown as well. In Syria, exam-related shutdowns were imposed for multiple years (Bischof et al., 2023), in order to prevent cheating in exams (Moinuddin, 2021).

3.3 Effect of Internet Shutdown

Empirical research also examines the effects of internet shutdowns. Internet shutdowns impact citizens' daily activities that require internet access, such as checking work emails, using ridesharing apps, job seeking, and accessing banking systems. Additionally, shutdowns can disrupt payments for essential services, such as e-banking, medical treatment appointment systems, and the healthcare system itself (Feldstein, 2021; Grinko et al., 2022; Marchant, 2020; Moinuddin, 2021). This disruption also obstructs communication, access to information and engagement. For instance, during Sudan's shutdown, the use of social media and global Google Web searches dropped significantly (Chatterjee, 2019; Marchant, 2020; Ngangum, 2023; Rydzak et al., 2020; Shah, 2021). Moreover, regions with higher internet penetration rates experience more severe negative impacts (Feldstein, 2021; Marchant, 2020). Additionally, shutdowns hinder educational opportunities for local youths. For instance, students cannot access online education platforms, apply for fellowships, or participate in online educational programs (Moinuddin, 2021).

Beyond individual effects, shutdowns also have national financial and economic impacts, from small businesses to overall GDP (Grinko et al., 2022; Marchant, 2020; Wagner, 2018). Feldstein (2021) states, "In 2019, at least 213 shutdowns occurred in more than thirty-three countries, leading to a cumulative economic cost of approximately $8 billion" (p.35). Some countries like Iraq, Sudan, India, and Venezuela registered losses in the billions due to their shutdowns (Feldstein, 2021). These losses are even more significant in countries where the economy heavily relies on the technology industry.

Internet shutdowns also affect the flow of information, disrupting citizens and protesters from accessing time-sensitive information (Bhatia et al., 2023). This disruption can impact freedom of speech and contribute to the spread of disinformation and misinformation. Without the internet, verifying information becomes challenging, often leading to the spread of misinformation and government propaganda. For example, during Sudan’s shutdown during the Khartoum massacre in 2019, there were conflicting reports about the death toll. The Ministry of Health claimed that only 46 were killed, while a member of the ruling

Sudan's Transitional Military Council announced that 13 people were killed (Bhatia et al., 2023). With the internet down, journalists and citizens could not verify the correct number.

Moreover, internet shutdowns often occur during social movements, affecting not only daily communication and entertainment but also the protests themselves (Grinko et al., 2022). Protesters cannot look at social media for upcoming actions and have restricted communication as phone calls and SMS are often surveilled by the government. Beyond immediate communication disruption among protestors, shutdowns can also threaten civil society leaders, weakening protest movements in the long run (Chari, 2024). An example of this occurred in the state of Kashmir in India. During nationwide protests against the Citizenship Amendment Bill in 2019, the government initiated one of the most prolonged internet shutdowns (Shah, 2021).

Literature emphasises that access to information and freedom of expression are fundamental human rights that should always be available, even in emergency situations (Chari, 2024; Vargas-Leon, 2016; Rydzak et al., 2020), as UNHRC also condemned them as human rights violations (Chatterjee, 2019). Hence, the nature of internet shutdowns harms human rights.

3.4 Shutdown Circumvention

Despite the power of internet shutdown, people around the have been trying to iterate new ideas to circumvent and overcome the limitations imposed on their internet access (Bhatia et al., 2023; Feldstein, 2021). While literature mainly focuses on the existing internet shutdown, including its trend, pattern and effects, some studies also touch upon the different methods protesters use to circumvent shutdowns in various regions. These methods, both technological and non-technological, involve circulating information on how to bypass the shutdowns and maintain communication within pre-existing social networks. (Bhatia et al., 2023; Rydzak et al., 2020). These circumvention tactics vary, depending on the scope of the shutdown, such as speed and duration, as well as the cultural and political context in which the shutdown occurs.

3.4.1 Non-Technological fix

One of the most frequently mentioned points in literature is the importance of neighbourhood committees and their respective local knowledge. Indigenous structures of

knowledge, cultural and social norms, and other local resources are effective in forming offline practices to communicate and mobilise during an internet shutdown. (Bhatia et al., 2023; Feldstein, 2021; Rydzak et al., 2020; Shah, 2021). On top of that, journalists also transmit data physically with a hard drive. For instance, some journalists in India have written stories on the ground, stored them on thumb drives, booked flights to Delhi or elsewhere to access the internet, and then sent emails to the respective organisations (Vargas-Leon, 2016).

3.4.2 Technological Fix

In terms of technological approach, studies have documented the use of various technology tools to bypass a shutdown, especially where the government does not block all access or where there are loopholes. Bhatia et al. (2023) have pointed out an essential point that internet shutdowns are sometimes "never complete or absolute, and there is always a gap in the system" (p.1111), and Shah (2021) also observed in the case of India that digital shutdowns are leaky, with loopholes and back doors that allow for the flow of information.

One of the popular tools is the use of a VPN, proxy servers or GPS spoofing applications that change users' locations outside of the shutdown area and bring data to their devices were recorded (Bhatia et al., 2023; Grinko et al., 2022; Shah, 2021). In Russia and Iran, new proxy servers via the MTProto Proxy website were being heavily relied on (Grinko et al., 2022). Some scholars also collected data of people using an "internet dongle", which is a mobile data connection hotspot where someone with internet access or with an international SIM can share their data to create an ad hoc network for communication (Bhatia et al., 2023; Shah, 2021). For example, in Iran, citizens in the border regions got mobile data connectivity via SIM cards from neighbouring countries and shared the data with their neighbours (Grinko et al., 2022). Some citizens in India also have access to broadband connection tied to landline telephony to obtain connectivity (Shah, 2021; Vargas-Leon, 2016).

Besides re-gaining internet access, some protesters also focus on documenting news events and sharing information. Protestors often use documentation applications like Tella and eyeWitness to encrypt and store images and footage on their phones. They wait until the shutdown ends to prevent security forces from identifying this information during questioning (Bhatia et al., 2023). According to Vargas-Leon's (2016) research, journalists in

Kashmir, India, write stories on the ground, store them on thumb drives, and then travel to cities with internet access to submit the stories to their respective organisations. Similarly, citizens in Iran use a satellite TV-based application called Toosheh. This app broadcasts Persian-language content and utilises file-casting technology (Grinko et al., 2022).

On the other hand, in cases where the internet is completely shut off, other tools that have been used include instant messenger applications that do not require internet, such as Bridgefy and FireChat, which use peer-to-peer mesh networks, or Briar, which relies on Bluetooth (Bhatia et al., 2023; Grinko et al., 2022; Shah, 2021).

3.4.3 Seeking External Help from Human Rights Organisations

Literature highlights different approaches that protesters who have experienced internet shutdowns use to prevent future occurrences while managing the current situation. One of the approaches is to advocate for a more transparent state communications protocol to bridge asymmetries of information. This can be achieved through counter-speech, i.e., posting accurate information on social platforms like Twitter and Facebook. Advocates also appeal to intermediaries, such as social platforms, to reinforce measures to curb misinformation through detection tools powered by artificial intelligence. They also urge these platforms to collaborate with independent fact-checkers and strictly enforce content policies and community guidelines (Chatterjee, 2019).

Digital rights advocates also promote anti-shutdown measures through legal approaches. Legal experts and advocates in countries such as Cameroon, Chad, Togo, and Uganda have collaborated with regional or international civil society organisations and taken up litigation against shutdown orders (Rydzak et al., 2020). Among these lawsuits, one in Zimbabwe was successful in having the shutdown declared illegal by the country's high court (Rydzak et al., 2020).

Existing literature also highlights local advocates' action of seeking international help. For instance, advocates would try to raise international awareness in order to put international pressure on the government to stop the internet shutdown (Grinko et al., 2022). Marchant (2020) also pointed out that despite international policy discussions on internet shutdowns, those in government, who are responsible for managing elections, protests, and other events often linked to internet shutdowns, seldom participate in these discussions.

3.4.4 Constrain of Combatting internet Shutdown

Despite protesters and journalists in various regions adopting creative ways to circumvent internet shutdowns, most remain disconnected (Grinko et al., 2022). Literature highlights common barriers to these circumventions. A key issue is that citizens are often not well-informed or educated enough to know the available tools or workarounds. Additionally, given the importance of local community networks in circulating information, some people are simply not well-connected enough, or there may be legal or political risks to sharing such information. Furthermore, some journalists lack technical expertise, making it difficult for them to understand how the internet works (Vargas-Leon, 2016).

Furthermore, the literature also indicates that these counter-appropriation activities often have limited capacity and can be costly, such as purchasing international SIMs (Grinko et al., 2022). Some methods carry high risks; for instance, connecting via foreign VPS in certain countries could be viewed as suspicious and potentially tracked by authorities. Additionally, some tools are not as well-designed as anticipated and can be rather ineffective (Grinko et al., 2022). There are also factors beyond citizens' control. For example, internet shutdowns are not always predictable, and citizens are often unprepared when they occur. By the time it happens, it is too late for them to quickly find alternative measures without access to the internet (Grinko et al., 2022).

3.4.5 Literature Review Conclusion

Existing literature on internet shutdowns predominantly focuses on their patterns, triggers, and impacts. While the minority of existing research provides insights into various circumvention tactics and empirical experiences in circumventing internet shutdowns, it mainly addresses the topic from an activism perspective for protesters. Very little literature focuses on circumvention strategies for journalists, addressing the media’s specific needs and situations in maintaining their reporting activities. Moreover, these discussions on shutdown circumvention are often brief and lack depth.

Therefore, this research aims to fill this gap by examining journalists' specific strategies to circumvent internet shutdowns.

4. Methodology

4.1 Data collection and sampling

The ultimate goal of this research is to gain a comprehensive understanding of actionable recommendations for journalists during shutdowns to sustain their work, exchange and disseminate information, and ensure citizens' rights to knowledge without internet connectivity, This will be achieved by examining empirical practices, first-hand experiences of journalists and technologists, and existing technology and advocacy work, addressing the following research questions:

RQ1: How do journalists currently cope with internet shutdowns?

RQ2: What are the best ways for journalists to cope with internet shutdowns to sustain journalistic work?

Therefore, a qualitative approach was adopted in this research. Creswell (1998) suggests that the qualitative method is good for the purpose of exploring an issue and providing a deeper understanding of a topic by examining its underlying meanings. Given the novelty of internet shutdowns and the limited systematic insights provided by existing literature, a qualitative approach could enable a better understanding and evaluation of internet shutdown circumvention through first-hand experiences. On the other hand, quantitative methods are not suitable for this research as it focuses on numerical data and statistical analysis, which may not capture the complex and nuanced experiences of individuals in different geographic locations.

The research process was divided into two segments: 1) semi-structured interviews with three technology experts specialising in different aspects of internet and press freedom, and 2) semi-structured interviews with eight journalists who have worked under internet shutdowns presented as case studies. The reason for including both experts and journalists is that combating internet shutdowns is often seen as a collective effort. As Creswell (1998) says, interviews allow researchers to collect more in-depth and comprehensive data as they give participants the opportunity to freely express their thoughts, feelings, and experiences in detail, at the same time enabling researchers to dip deeper into interesting responses, clarify misunderstandings, and discussion would emerge during the conversation. Therefore, interview approach is suitable for achieving a more comprehensive perspective on the topic

by including experience and opinions of different stakeholders and to subsequently exploring the disparities between expert recommendations and innovations, as well as the practical usage scenarios faced by journalists on the ground.

4.1.1 Interview with experts

A purposive sampling data collection method was employed for interviews with experts. This approach aims to gain in-depth insights into specific aspects of internet shutdowns by selecting participants with relevant experience in the field (Mason, 2002).

The three experts below were selected:

Table 1: Expert Interviewee Information and Specialties

Interviewee	Position and Affiliation	Specialties and Covered Topics During the Interviews
Felicia Anthonio	The #KeepItOn Campaign Manager at Access Now, a global campaign fighting against internet shutdowns worldwide (Access Now, 2024).	- General information about internet shutdowns - Prediction of trends in internet shutdowns - Experience, skills, and obstacles in anti-internet Shutdown advocacy - Observations, reflections, and advice on working with technologists
Shoeb Md Abdullah	Founder of Activate Rights, a voluntary initiative focused on internet freedom and the anti-shutdown movement in Bangladesh (Activate Rights, n.d.). Network Measurement Fellow in OPTIMA Project, Internews' program that supports collaboratively developed	- Available tools and countermeasures for internet shutdowns - Experience, skills, and obstacles in shutdown circumvention training and advocacy - Opinion and advice for international communities

	resources to enable better responses to major instances of internet shutdowns in Africa (Internews, 2023).	
Michael Rogers	Founder of Briar project, a peer-to-peer encrypted messaging app with no internet access required (Briar, n.d.).	- Information and usage of peer-to-peer messenger tools - Promoting and educating journalists on shutdown circumvention tools - The technological side of internet shutdown and circumvention - Experience in developing shutdown circumvention tools as a technologist

The interviews for experts began with four structured questions related to the challenges journalists face in shutdown areas, how the international communities perceive their work, be it advocacy or technical innovation, and the obstacles they face when combating internet shutdowns. Follow-up questions were asked throughout the structured interview. Afterwards, a different set of pre-designed questions was used for each participant, tailored to their respective expertise as listed in Table 1.

4.1.2 Interview with Journalists

For interviews with journalists, a snowball sampling data collection method was employed as it is particularly suitable for investigating sensitive issues and participants were recruited through referrals (Biernacki & Waldorf, 1981). Internet shutdowns predominantly occur in authoritarian countries (AccessNow, 2020), where journalists face legal risks from governments. Thereby, journalists in such contexts may not feel safe revealing information about their work without a reliable referral source. The research sorted out interviewees on different channels: broad inquiries requesting respondents were distributed on 1) the Slack

channel of the Open Observatory of Network Interference (OONI), 2) the Signal group of the internet Shutdown Mentored Training Program hosted by the Advocacy Assembly; 3) personal contacts of the researcher in journalism and the digital rights communities, and 4) the Facebook group of Alumni of the Erasmus Mundus Master's in Journalism, Media and Globalisation. Then, through these initial contacts, additional individuals were identified, and direct outreach was conducted.

The interview began by asking about their personal experiences with internet shutdowns, including background information and a description of the specific occurrences. This was followed by questions about their experience working during the shutdowns and their experiences with employing circumvention tactics. An open-ended question also encouraged reflections on potential future shutdown occurrences. Lastly, the interviewees addressed their views and advice on current technology and international communities. Follow-up questions were asked throughout the structured interview.

4.2 Analysis

Most interviews, except one, were conducted using either WhatsApp, Signal, or Jitsi, all end-to-end encrypted messaging tools, based on the interviewees' preferences. The audio interviews lasted between 46 and 84 minutes and were conducted between March 14th and July 2nd of 2024. The interview with M. Rogers, the founder of Briar, was conducted in written form via email, as per the interviewee's preference due to the language barrier.

Most interviews, except one, were carried out in English. The interview with J1_Kazakh journalist was conducted in Russian, with the presence of an interpreter to translate on the spot. With the participant's consent, all audio interviews were audio-recorded and transcribed using GoodTape—a fully encrypted AI transcription tool with a data retention policy that ensures immediate deletion after transcription (Klitgaard, n.d.). This approach was adopted to safeguard the security of the interviewees. All follow-up questions were asked via text form through email, WhatsApp, or Signal, depending on the preferred communication method.

In order to interpret the data, this research opts for content analysis. According to Krippendorff (2019), content analysis allows the researcher to analyse and identify patterns, themes, or trends by measuring the presence, frequency, and intensity of specific words or themes within a set of relatively unstructured data. Content analysis is suitable for this

research because the interviewees are from different continents and political contexts, and they represent various fields such as journalism, digital rights, and technology. Content analysis can help identify common threads in their thoughts to formulate a unified conclusion on how journalists can cope with internet shutdowns.

The transcripts, after removing all identifying information or off-the-record content, were uploaded to MAXQDA software for coding and analysis. An inductive coding approach was used. During the coding process, the interviews were read repeatedly to gain an overall understanding of content related to the research aim. They were then annotated with initial codes that captured key concepts, themes, and patterns as they emerged from the data, continuously refining and adjusting them as new data was analysed. This approach helped combine the data into broader themes and theoretical dimensions (Chandra & Shang, 2019). Then, a content analysis was conducted to systematically categorise the data, and identify recurrent themes and narratives, as well as new insights that were not frequently mentioned in existing literature among interviewees.

To address safety concerns, the identities of the journalist interviewees remain anonymous in the analysis and are indicated by their respective interview numbers, along with their country and position: J1_country & position.

5. Findings

5.1 Main Challenges Journalists Face During Internet Shutdown

Interviewees raise different concerns and challenges that they face during internet shutdowns. This section will explore three primary challenges: communication obstacles, difficulties in conducting research, and increased oppression targeting media from governments. By examining these issues, the measures needed to address them could be more effectively explored.

5.1.1 Communication Challenges During Internet Shutdowns

Modern communication heavily relies on internet-dependent methods, such as messaging apps like WhatsApp and Signal, or online file transfer services like WeTransfer, especially in the journalism field (Bivens, 2008; J1_Cameroonian TV journalist, personal communication, May 27, 2024). Journalism is a collaborative endeavour, often involving

multiple roles such as editors, social media editors, and field journalists to finish a story. However, during an internet shutdown, interviewees noted extreme difficulties in communicating with their coworkers and that they struggled to receive instructions from editors or send news material back to the newsroom promptly.

> "So the only challenge that we had was: for me to send the articles to the editor on time. Because…we send our work using the internet" (J1_Zambian journalist, personal communication, May 20, 2024).

Even if journalists manage to file a story, another challenge caused by the disruption of communication that journalists face during internet shutdowns is the hindrance in delivering stories to audiences, which could lead to confusion among the audience.

> "The main challenge for me was sending my story. I know how people wait for my prime-time news. And then prime-time news comes, I'm not there because there's no internet" (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

5.1.2 Difficulties in Conducting Research and Fact-checking Due to Media Blackout

Internet shutdowns often lead to a media blackout, to some extent if not fully, preventing media from conducting journalistic research online, which has become a crucial part of journalism nowadays. As interviewees have expressed, this directly affects the quality of journalistic work.

The obstacle of conducting research affects journalists based in rural areas more intensely due to the inability to travel to locations to collect information. Rural areas often lack the resources to conduct research locally and physically. They also do not have the alternative of travelling to the capital to conduct research because of potential imposed curfews that come with internet shutdowns. J1_Zambian journalist mentioned that, as a journalist based in a rural area of a developing country, she often has limited access to libraries and other materials from media institutions, unlike those based in the capital.

> "Internet shutdowns affect the quality of journalism because when we are doing a story, like for me, my research has to be online. So for me to do a story, I have to use the internet to research and know what is happening in the country through online

sources or through Facebook and by searching other media institutions' pages to read" (J1_Zambian journalist, personal communication, May 20, 2024).

Fact-checking is also a significant problem as the media ecosystem becomes decentralized and increasingly reliant on citizen journalists for footage (Carlson, 2016). During internet shutdowns, it becomes nearly impossible to circulate news footage or photos uploaded by citizen journalists or other media outlets, leading to a lack of access to reliable information sources.

> "An example that happened in Mahshahr, which is a city in southern Iran. Reports say that hundreds of people were rounded off first by security forces and then shot at and killed right in the same spot. But nobody can confirm that because we only have a few videos that people shot as it was happening and later released" (J1_Iranian independent journalist, personal communication, March 14, 2024).

This problem affects independent journalists more significantly as they work alone, without a team of coworkers to collaborate with or the resources of a newsroom to support them. J2_Kashmiri freelance journalist also pointed out the problem of not having a press card, as she does not belong to a registered news organisation.

> "What they [journalists in legacy mainstream media] would ideally do is they would collect some kind of petrol or, you know, three, four colleagues would come together, share a small car, and then come back. Now, me as a freelancer could not afford that" (J2_Kashmiri freelance journalist, personal communication, May 30, 2024).

As a result, both J1_Iranian independent journalist and J2_Kashmiri freelance journalists mentioned that they simply stopped filing any stories or reporting because they could not "really interact with the world" (J1_Iranian independent journalist, personal communication, March 14, 2024).

5.1.2 Lack Of Knowledge Regarding internet Shutdown

Another big obstacles for journalists to react to internet shutdowns properly is that almost all shutdowns are unannounced, despite some being predictable. They happen suddenly, leaving journalists confused and paralyzed both emotionally and practically.

> "We had no idea. We did not see it coming. It's something we didn't expect; it's something we weren't trained to deal with. We weren't prepared for this" (J1_Egyptian news agency journalist, personal communication, May 21, 2024).

Even in cases where shutdowns are predictable, many aspects remain unforeseeable, such as the scale, duration, or whether it will be a social media blackout or a full shutdown, making it harder for journalists to prepare. Additionally, interviewees pointed out that shutdowns are often phased, complicating the situation further. For instance, in Iran, there was a period when home broadband and Wi-Fi worked, but mobile data did not (J1_Iranian independent journalist, personal communication, March 14, 2024). Similarly, in Zambia, the government shut down the internet in phases, starting with the internet and then proceeds to blocking cell signals (J1_Zambian journalist, personal communication, May 20, 2024).

Moreover, journalists often lack technical knowledge about internet shutdowns. For example, an interviewee did not know the exact definition of different types of shutdowns such as "throttling". This lack of knowledge makes the already complicated situation more difficult to identify or comprehend, leaving journalists struggling to figure out what's happening or confirm a shutdown is occurring.

As mentioned in literature review, interviewees further pointed out that this ignorance also leads to low incentives to combat shutdowns, whether through learning about circumvention methods or advocating against shutdowns, leaving journalists even more unprepared.

5.1.3 Increase Oppressiveness Targeting Media from Governments

Internet shutdowns often occur under broader oppressive conditions, such as curfews and police stop-and-search (M. Rogers, email communication, May 27, 2024). In many cases, governments shut down the internet to prevent the media from spreading information, and therefore, they simultaneously employ various oppression tactics specifically against journalists, such as the use of military or police brutality (F. Anthonio, #KeepItOn Campaign Manager, personal communication, May 2, 2024).

> "There tends to be a crackdown on media…you know, newsrooms being raided or journalists being arrested, journalists being threatened, intimidated. These kind of

things tend to happen during these times [during internet shutdowns]" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

J2_Kashmiri freelance journalist highlighted that female journalists face greater risks due to their cultural backgrounds, stating, "Women were targeted by security forces and other agencies" (J2_Kashmiri freelance journalist, personal communication, May 30, 2024)". Another example involves increased scrutiny and the use of spyware, which adds the threat of digital compromise to the challenges of dealing with an internet shutdown (J1_Kashmiri online news journalist, personal communication, May 23, 2024).

Although international and technology communities are making increasing efforts to develop workarounds for digital authoritarianism, governments are concurrently improving their oppression strategies. For human rights organisations and journalists, continuously finding sustainable and effective countermeasures against these ever-evolving tactics remains a significant challenge.

> "If you shut down the internet, maybe you're taken to court, and the closest thing that happens is the government is ordered to pay the filing fees or legal fees, but there's no real punishment for governments that shut down the internet. I think we [digital rights communities] have made a lot of progress in raising awareness, and having different resolutions from the UN, the African Commission, and other places denouncing internet shutdowns. But I think governments are just becoming more and more repressive" (F. Anthonio, personal communication, May 2, 2024).

5.2 Technological Solution for Journalists

Interviewees pointed out several technological solutions they have adapted during shutdowns in order to maintain journalistic work, by either gain access to the internet, or to maintain communication. It includes the use of tools and applications, readapting older technologies, and seeking solution for alternative internet.

5.2.1 Use of Virtual Private Network (VPN)

Echoing what existing literature stated, VPN use is one of the most commonly mentioned solutions to combat internet shutdowns. All interviewees stated that they installed a VPN after experiencing their first internet shutdown.

However, VPNs only work for certain types of shutdowns due to the nature of VPNs tunnelling over the public internet, which requires an internet connection to access a VPN server (Ferguson & Huston, 1998). As Anthonio explains, VPNs "normally work during partial disruptions" (personal communication, May 2, 2024), such as social media shutdowns. Therefore, they are not a solution during a full blackout, as during complete internet shutdowns, users are "not actually able to do anything using the internet" (personal communication, May 6, 2024), as Abdullah stated.

A full blackout could be hypothetical because, as mentioned in the literature review, in reality, internet shutdowns are often flawed and not complete blackouts. There may be instances when the internet is available in specific buildings or temporarily comes back on. In situations like this, a VPN is very useful to bypass the internet shutdown.

> “Usually, the embassies or the American embassy or the UN headquarters or the UNOCA compound (United Nations Regional Office for Central Africa), they will have internet... because they have their own satellites. And then later on, we found out that there were also certain banks who were able to access the internet” (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

In situations like this, a VPN can be an effective tool for circumventing the internet shutdown.

> “I connected to a VPN when I was in the office [where the internet was available]. But sometimes I connected at home. For example, 24 hours a day, 22 of them are without the internet, but sometimes they turn it on for an hour. And at this moment, you could connect quickly and then save this connection after this hour of the internet runs out” (J1_Kazakh journalist, personal communication, May 28, 2024).

However, flawed shutdowns are often not announced, or information is only circulated within a small, trusted circle. Journalists often do not know when the internet will be restored or where it will function, which makes it difficult to devise a plan to take advantage of any loopholes (J1_Kazakh journalist, personal communication, May 28, 2024).

Moreover, many types of VPNs are available that require different functional requirements and construction methods, not to mention different brands with varying qualities and costs. So, whether a VPN works well during a shutdown also depends on the

quality of the VPN provider available in the region. Iranian journalist expressed that "stronger VPNs that would work uninterruptedly" could potentially be useful during shutdowns (J1_Iranian independent journalist, personal communication, March 14, 2024).

Another consideration is the legality of VPNs in addition to their technical aspects. Various countries have put restrictions on VPNs, such as banning them or removing them from app stores. For example, in Iran, only government-approved VPNs are allowed (Sinaiee, 2024), which might be monitoring the traffic and will not be useful when the government intentionally shuts down the internet. In Turkmenistan, Belarus, and Iraq, VPNs are banned, and the government enforces this rigorously (Danao, 2023). In such cases, using a VPN might not be a feasible solution for obtaining internet access, even if it technically works, as journalists must also consider the associated risks and potential consequences.

5.2.2 Use of Offline Instant Messenger Tools

The literature review and news reports show that offline instant messenger were frequently discussed among researchers and activists. Among related tools that are currently available on the market, Briar and Bridgefy are two of the most popular (Beh Lih Yi, 2021; Linow & Freund, 2022). Briar is a messaging app that uses peer-to-peer (P2P) technology, enabling users to connect directly within a range of about 10 meters via Bluetooth or Wi-Fi without accessing the internet (Briar, n.d.). Bridgefy is another messaging app that allows users to communicate through a mesh network established via Bluetooth and Wi-Fi, with a reach of around 90 meters (Albrecht et al., 2021).

However, almost all interviewees have never heard of these tools. One reason for this could be the differing needs of activists and journalists. Activists aim to communicate with each other and spread information directly, where the short-reach feature of the app remains a limitation but is still useful in certain situations. In contrast, journalists need to communicate with various parties in different locations and send images and footage for reporting, where the reach limitation presents a more significant obstacle.

Another possible reason is the varying environments and situations. Abdullah, as a technology trainer, noted that, despite the importance of mesh networks in circumventing full blackouts or throttling, in Bangladesh, mesh networks are not the best option:

> "Because it's a mesh network, you need to stand at a certain point. But at the protest site, it doesn't happen because police are always hunting people, so you need to scatter" (S. M. Abdullah, personal communication, May 6, 2024).

Another factor is that these tools or applications on the market are not very user-friendly. Abdullah suggested that those tools "need to update their interface and improve their advocacy" (S. M. Abdullah, personal communication, May 6, 2024).

However, J1_Ethiopian newspaper journalist found peer-to-peer instant messaging potentially useful despite hearing about it for the first time during the interview, particularly the feature of sending image attachments, which facilitates easier image transfer within the newsroom. This feature is available in Briar (Briar, 2021).

> "I think that being able to share files [is useful], for example, like when we use SMS here in Ethiopia, it's just SMS, just text, that's all you can send. You cannot share files, you cannot send photos, you cannot do anything else…. So I think it's really a step up from that" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

Another messenger tool mentioned by Anthonio and the J1_Cameroonian TV journalist is "SMSWithoutBorders (SWOB)," a messaging app that allows encrypted messages to be sent to online platforms such as Telegram, Gmail, and Twitter without an active internet connection through a network of SMS gateways (SMSWithoutBorders, 2023). However, the Cameroonian journalist was not able to provide more insights into his experience, and it was not mentioned by other interviewees. Therefore, this method requires further examination.

5.2.3 Readapting Legacy Communication System

In addition to new technology, all interviewees commonly mentioned that their news organisations reverted to using legacy communication technologies that do not require an internet connection, specifically, cellular communication such as SMS, landline phones, and fax machines to communicate with others both within the country and internationally.

> "I was checking state media other media what they were saying, and then taking whatever … information she [the colleague] was bringing, and write it down, and either phone through a landline colleague abroad or … we would also fax it to one

of the offices and they would publish" (J1_Egyptian news agency journalist, personal communication, May 21, 2024).

Another suggestion mentioned in the literature review was the use of an international SIM card, which was also brought up by Anthonio. An international SIM card is a SIM card obtained from an ISP in a country other than the user's current location. It allows the user to connect to foreign networks through a series of global interconnections and agreements between ISPs via roaming (Miller, 2023). For example, according to news reports, in Iraq and Sudan, citizens have used international SIM cards during internet shutdowns, though feedback indicates they are expensive and the signal is often weak (Bhalla, 2021; Collins, 2019). Most interviewees had not heard of this method but showed interest in it, despite expressing concerns about the cost. Thus, it could potentially be a way to bypass internet shutdowns, depending on the technical methods used by authorities to shut down the internet and whether the infrastructure is functioning.

However, the constraint of cellular communication is that it is unsecure, as it is unencrypted (Peeters et al., 2022). For example, both SMS messages and landline calls are not end-to-end encrypted, meaning they can be intercepted and read or listened to by third parties, including mobile network operators, and government agencies. Countries that impose internet shutdowns often intensify their surveillance and digital control over journalists and citizens, this can pose a risk for journalists and their contacts, or create a sense of insecurity and distrust.

> "The conversations that you have [on landline] are not going to be secure. So the questions you ask will also be determined by the level of security you feel using phone lines…Somebody cannot tell me things that are off the record on a phone line" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

5.2.4 Satellite Technology as an Alternative Source of Internet

Most interviewees expressed that the ultimate solution to combat internet shutdowns might be alternative internet technologies. Multiple interviewees also mentioned satellite technology. Satellite internet can bypass traditional ISPs as the signal communicates directly with satellites orbiting the Earth instead of using terrestrial cables and infrastructure (Maini & Agrawal, 2007).

J1_Egyptian newspaper journalist mentioned that as early as 2011, during the Arab Spring, journalists in Egypt had used satellite phones to transfer news footage (personal communication, May 21, 2024).

Starlink, a satellite internet constellation operated by SpaceX, a company founded by Elon Musk, began providing internet services through its public beta program called the "Better Than Nothing Beta" in October 2020 (Grush, 2020), offering intermittent connectivity. The service was gradually expanded to countries where traditional internet is not always available, including Zambia and Ukraine (Faboade, 2024; Tobin & Borak, 2022). As Starlink's service became popular, journalist and technologist interviewees expressed that it is potentially a good alternative source of internet.

> “With the emergence of something like Starlink or Elon Musk, I think it would be difficult to shut down the internet completely because this is a satellite” (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

However, one of the problems with satellite internet is that it is still centralized, meaning users depend on the provider's business decisions and government regulations. For instance, Starlink announced it would remove its services in Sudan by restricting roaming in jurisdictions where it was not licensed in 2024, which humanitarian groups described as risking the "collective punishment" of millions of Sudanese (Townsend, 2024). Technologists have expressed concerns about future government restrictions on satellite networks.

> “So satellite internet is very important to circumvent this kind of regular cable network stuff and the regular monopolized state-owned telecommunication stuff.… But the problem is that the satellite communication is monopolized by some business entity” (S. M. Abdullah, personal communication, May 6, 2024).

> “I think the use of satellite internet via unmodified phones could be very significant. If it works at scale, then I guess governments may try to restrict the availability of satellite-capable phones (e.g., by requiring phones to be network-locked to approved carriers)” (M. Rogers, email communication, May 27, 2024).

5.2.5 Building an Offline News Archive

J1_Ethiopian newspaper journalist mentioned that during the time of the shutdown, the newsroom she worked for had built an offline news archive. This archive allowed staff to search and read previous news articles or material without internet access, compensating for the inability to conduct research online.

> "During the internet shutdowns, we relied on a few things…. We have the old copies of the newspaper. But we have an archive where we can access offline, the older copies of the newspaper" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

5.3 Non-technological Solution for Journalists

Apart from technical solutions, interviewees also highlighted tricks, protocols or workarounds for maintaining journalism without access to the internet. This section will discuss the importance of building networks with different communities, and setting up contingency plans in advance.

5.3.1 The Importance of Building a Network, Both within the Community and Internationally

> "Anytime, anywhere, in any circumstances. If you're in a network, if you're in a group, it's highly important" (J2_Kashmiri freelance journalist, personal communication, May 30, 2024).

Interviewees echoed the importance and advantages of having a local neighbourhood suggested by existing literature. They pointed out that building a network with local media, the tech community, and other parties is crucial, as all journalists mentioned that they heavily relied on collaboration during times of shutdown, including knowledge sharing. J1_Zambian journalist stated that she, along with many other Zambians, learned about VPNs through people sharing this knowledge on social media right after the internet shutdown (J1_Zambian journalist, personal communication, May 20, 2024).

Journalists mentioned that the division of labour was essential to keep their work going, whether it was working as a team with other journalists or coworkers. J2_Kashmiri freelance journalist noted that, as a female, travelling alone was dangerous, especially during

an internet shutdown, so media workers in the region had to remain in groups and carpool together (J2_Kashmiri freelance journalist, personal communication, May 30, 2024) for security.

As mentioned, internet shutdowns are often flawed, so journalists emphasized the importance of building relationships with people who knows about insider information, such as government officials or ISP staff, to obtain insider information related to the shutdown, such as places where the internet would still be available.

> "I think a few of the people who are really established journalists did have contacts within the police department or other government places. They used those contacts to send information, but it was completely hidden" (J2_Kashmiri freelance journalist, personal communication, May 30, 2024).

> "I would try to make friends with some guys working at the telecommunication company. There's always a way out… People who have a relative working in state corporations knew how to go about and have access to the internet" (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

J1_Ethiopian newspaper journalist also highlighted the importance of building connections with local news outlets, especially for freelance journalists. This provides an alternative way to publish their work when it is difficult to reach out to international outlets via the internet.

> "As a freelancer… having a good relationship with the local outlets is a good advantage because, you know, you can collaborate with them during the times when you can't work with your other editors. …if your employers are international outlets and you are facing an internet shutdown, that means you can't pitch stories to them" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

5.3.2 Importance of Setting Up Contingency Plans in Advance

Although no government announces shutdowns in advance, journalists noted that shutdowns are sometimes predictable, occurring during significant conflicts or special events such as visits from foreign politicians or national holidays. Therefore, preparing for shutdowns and planning the division of labour is crucial. Interviewees pointed out that journalists often only start looking for alternatives after realizing the internet is out.

However, they reflected and strongly suggested that media organisations should develop plans in advance.

> "But as an institution and as media houses, there needs to be a protocol for …what are the procedures when you face an internet shutdown and how do you work within those conditions? In the newsroom that we had, which is a newsroom is one of the oldest newsrooms in the country, and we did not have such a procedure" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

Journalists currently rely on physical movement to replace internet traffic, either to gather or publish information. J2_Kashmiri freelance journalist expressed that she "would have done things differently" if another shutdown occurred (J2_Kashmiri freelance journalist, personal communication, May 30, 2024). Therefore, planning the workflow in advance, whether working alone or as part of a team, could potentially decrease panic and enable journalists to resume work efficiently and rapidly.

> "The only issue I had was sending stories back to the central newsletters… I had to travel to the neighbouring region [where the internet was available] to send news out there. So I took inter-urban transport, went to another region, that's another state. And then I had to go to a cyber cafe, buy time there, and then use my USB. And then I sent the story. It was really stressful" (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

> "We journalists were already developing our own tactics of how to work. Someone took the material, ran a few blocks further into the internet access zone and transmitted photos and videos to the editorial chat from there. And while he was running away, his colleague was missing, so he continued to shoot events in place. When he came back, it was his turn to run a few blocks further until the internet appeared and send materials there" (J1_Kazakh journalist, personal communication, May 28, 2024).

Sometimes, larger-scale teamwork or help from others is a necessity rather than a convenience.

> "I would not waste time going to the media centre. I would rather report two, or three days later, collect all the information, write my copies, put it on a hard drive, go to

the airport, and give it to somebody and tell them, 'Could you please pass it on to my editor?" (J2_Kashmiri freelance journalist, personal communication, May 30, 2024)

"After a couple of days, they had certain bank headquarters to access the internet. So we pulled our connections [to find out where internet was available]. And our editor-in-chief would go to the banks, would go to a certain bank where they had internet, and she would collect questions from everybody in the newsroom, what we wanted to check, what kind of database we wanted. And then she would go there, spend a couple of hours researching and looking up the things that we had asked her, and then she would come back with the answers" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

5.3.3 Working with And Building Connections With Diaspora Communities

Another suggestion made by interviewees was to work with diaspora groups. Authoritarian countries where shutdowns are imposed often lag in technological development, meaning citizens are delayed in learning about new technologies. In contrast, diaspora communities have migrated to more developed countries, and they understand the needs and political context of their home country. They can act as a medium to introduce available tools, or to assist in making workarounds work during a shutdown. More than one journalist stated that they learned about VPNs through diaspora communities.

"There was one Kazakh who lives abroad. He provided this traffic through a proxy server, through Telegram. And people could connect then" (J1_Kazakh journalist, personal communication, May 28, 2024).

5.4 Focusing on Recording and Archiving News Events Due to Lack of Solutions for Full Blackouts

"I think the biggest challenge for us remains navigating a complete internet blackout. Finding a solution is almost impossible" (F. Anthonio, #KeepItOn Campaign Manager, personal communication, May 2, 2024).

Among different types of internet shutdowns, a full blackout is particularly challenging to cope with. Some popular circumvention tools, such as VPNs, that are potentially useful

would not work under a full blackout. Journalists often “had no means to actually publish the news” (J1_Kashmiri online news journalist, personal communication, May 23, 2024) and could only “raise their hands and keep silent” (S. M. Abdullah, personal communication, May 6, 2024).

Although bypassing a full blackout is difficult, it is also crucial to spread the news afterwards, both for citizens' right to know and for advocacy outside the country. Multiple interviewees stated that there is often a delay in delivering news, but they still try hard to document events and send information once they get a connection or workaround (J1_Cameroonian TV journalist, personal communication, May 27, 2024; J2_Kashmiri freelance journalist, personal communication, May 30, 2024). Continuous sharing of information can be very helpful (J1_Zambian journalist, personal communication, May 20, 2024).

During shutdowns, especially those caused by uprisings or elections, authorities often implement strict security policies to control the flow of information, making it difficult for journalists to keep photos or footage of news events. Police may search journalists' phones and delete relevant data such as news footage, putting journalists at risk of legal repercussions or police brutality and loss of news material (J1_Kashmiri online news journalist, personal communication, May 23, 2024).

> “If I don't have internet, I probably do two things: I either risk taking the photo and coming home to send it to news organisations, or I just decide not to take the photo because if they take my phone and catch me with that image, I'll be in trouble” (J1_Iranian independent journalist, personal communication, March 14, 2024).

> “I would like to quickly send it before they detect and delete it. While travelling if security forces got a chance to access your documents or camera, they would destroy it” (J2_Kashmiri freelance journalist, personal communication, May 30, 2024).

This underscores the importance of archiving and creating backups in addition to trying to obtain connectivity. Just as existing literature stated, protesters also focus on documenting news events with documentation applications, which is a tactic journalists can also adapt. So far, interviewees have not provided much insight regarding protecting news materials. However, Tella, an mobile application mentioned in literature review that acts as a camera

or audio recorder that automatically encrypting and hiding files within the app,[3] claims to provide a solution for this issue. It also allows users to mask the app's appearance to bypass police searches (Tella, n.d.). None of the journalists had heard of Tella, but all expressed interest and found the idea extremely useful during internet shutdowns, as it would allow them to capture news events while reducing the risk of police detection.

> "Sometimes you can't send texts, cell phone lines are jammed, you can't call people…it would make communication easier as well. …I think that being able to share files. Because, for example, when we use SMS here in Ethiopia, SMS is just text, that's all you can send. You cannot share files, you cannot send photos, you cannot do anything else…. So I think it's really a step up from that" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

Therefore, Tella could be a potentially useful tool after further examination.

5.5 Leveraging Solutions in the Face of Varied Threats and Contexts

One of the common points of discussion emphasised by interviewees is that there is no one-size-fits-all solution to internet shutdowns, as each instance is unique and requires tailored responses depending on various factors. As Anthonio stated, a tool effective in Country A may not function similarly in Country B, even if the shutdown scenarios appear similar (personal communication, May 2, 2024).

First, how the government technically implements the shutdown and its scale can affect how effective a certain circumvention tactic is. For instance, if a government enforces region-specific shutdowns, an international SIM card could potentially bypass the blockage if the local mobile network supports international roaming. However, if the government opts for infrastructure-based shutdowns, all connectivity, including international roaming, would be affected, rendering international SIM cards ineffective in such cases.

Furthermore, the level of computer and technology literacy among journalists varies across countries, influencing the usability of certain tools. For example, in regions like Kashmir, some journalists rely on feature phones without internet access, making circumvention tools like VPNs unusable (J1_Kashmiri online news journalist, personal

[3] Tella is a tool developed by Horizontal, a nonprofit organisation that creates technology for human rights defenders. (Horizontal, n.d.)

communication, May 23, 2024). Even within the same countries, it varies from region to region. J1_Zambian journalist points out that journalists in urban areas are well-equipped and use newer technologies, while in rural areas, computer literacy is progressing at a much slower pace (J1_Zambian journalist, personal communication, May 20, 2024).

> "As the level of digital security awareness differs, so does the technology usage among journalists—from basic applications like WhatsApp to more secure tools like Signal or Thunderbird for encrypted communication" (F. Anthonio, #KeepItOn Campaign Manager, personal communication, May 2, 2024).

Another fundamental factor influencing the efficacy of solutions is the varying fundamental internet structures across countries. For instance, Iran operates its National Information Network (NIN), or "Halal internet," which is a government-controlled intranet with separate technical infrastructure, including servers, DNS services, and routing mechanisms (Anderson, 2012). This setup differs significantly from the global internet, affecting how circumvention during shutdowns is approached in Iran compared to other countries (Anderson, 2012).

On the non-technical side, political backgrounds lead to varying measures during shutdowns, such as police searches, curfews, and signal blockages, which can drastically impact the feasibility of circumvention tactics. And,This diversity in circumstances also affects journalists' needs differently. For example, during civil unrest, if SMS services are cut off alongside internet shutdowns, journalists may prioritize alternative communication methods. Conversely, if SMS remains available, their focus may shift to archiving news materials rather than communication needs.

The threats journalists face also vary significantly, even if a tool is technically effective and available, users may face severe legal consequences based on these contextual factors. For example, while VPNs might be widely used in some countries, Kashmiri freelance journalists note that VPN usage can lead to legal charges under strict laws like India's Unlawful Activities (Prevention) Act (UAPA) (J2_Kashmiri freelance journalist, personal communication, May 30, 2024). Similarly, Iranian journalists avoid using SMS due to surveillance concerns (J1_Iranian independent journalist, personal communication, March 14, 2024). Police practices such as phone searches to locate foreign SIM card users in Sudan, as noted by Felicia Anthonio, further illustrate the diversity of threats faced by journalists (F. Anthonio, #KeepItOn Campaign Manager, personal communication, May 2, 2024).

J1_Cameroonian TV journalist reports similar practices where police seize phones to search for incriminating evidence (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

5.6 Suggestions for Human Rights Organisations and Technological Communities

Apart from journalists on the ground themselves innovating tactics to circumvent shutdowns, many local and international human rights organisations, as well as technologists, have contributed to circumventing internet shutdowns, or to maintain press freedom. More than 300 organisations from over 100 countries around the world have joined the #KeepItOn campaign, an initiative launched by Access Now, a global non-profit organisation that advocates for digital rights and fights against internet shutdowns (Access Now, 2024; Tsandzana, 2023). Journalists and experts discussed the current shortcomings and future potential in this area, pointing out what human rights organisations can do to assist journalists to cope with internet shutdown

5.6.1 Providing Training for Local Journalists and Civil Society

To empower journalists with knowledge in internet shutdown circumvention and bridge the gap between circumvention tools and journalists in affected areas, international organisations can organize Training of Trainers (ToT) programs. As mentioned, some journalists have never heard of potential effective circumvention tools, or lack knowledge in coping with shutdowns. ToT programs involve teaching a small number of journalists or local civil society members who can then organize training for people in their local network to spread the knowledge. For example, Access Now has been conducting ToTs and localizing content such as tool tutorials into relevant languages.

> “Maybe they could have some members of the forum organize workshops, organize some promoting stuff because people do not know enough about Bridgefy or this kind of stuff” (M. Rogers, email communication, May 27, 2024).

> “Even here we don't talk about spyware, even though spyware is something we should pay attention to. A lot of journalists get their equipment confiscated regularly and it's something that we should pay attention to. But who's gonna talk about spyware? It's such a scary topic [for non-tech-savvy people]. …Somebody who can

speak on this and who can encourage people to speak about this [would be really helpful]" (J1_Ethiopian newspaper journalist, personal communication, July 2, 2024).

All interviewees find training sessions useful. However, Abdullah highlights one current shortcoming: Current training focuses on advocacy, "but there is no advocacy about when internet shutdowns happen, how journalists and activists are communicating with each other." Journalists do not use certain tools simply because they have never heard of them (S. M. Abdullah, personal communication, May 6, 2024).

> "A handbook or guide would be super helpful… not only for the international community but for local organisations to do that. I think there could be a handbook to prepare people, not only journalists because oftentimes you will see NGOs who come and support journalists" (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

> "It seems to me that the more education and promotion of journalists, the better. Because journalists will then share this information with the population, and the level of digital literacy will also grow… to understand what digital rights are, what they need to know, and how to protect their digital rights and cybersecurity" (J1, Kazakh journalist, personal communication, May 28, 2024).

Such ToT programs not only equip journalists with knowledge but also act as a bridge to connect local media with different organisations for future collaboration and support (J2_Kashmiri freelance journalist, personal communication, May 30, 2024).

One thing to bear in mind is that international communities should shift their focus to rural areas as well instead of only focusing on main cities. J1_Zambian journalist observed this phenomenon and suggested organisations host virtual sessions so people who are not located in the capital and who are more disadvantaged during shutdowns could also participate online.

Both the Zambian and Cameroonian journalists mentioned the forgetfulness of citizens and noted that "there's no continuity in what advocacy communities are doing" (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

> “Some of us just had to learn things here and there. And I think after a few years, we forgot about it. We forgot how to navigate through all these things” (J1_Zambian journalist, personal communication, May 20, 2024).

Therefore, they highlighted the importance of continuous effort rather than one-off training. This can also address the rapidly changing political environment and the growth of both circumvention and oppression tools.

In addition to training programs for journalists or specific targets, public educational programs were also suggested by interviewees. With financial resources, advocacy communities can “make training available like easy, easy things for normal people” (J1_Egyptian news agency journalist, personal communication, May 21, 2024). As J1_Cameroonian TV journalist suggested, advocacy communities can seek financial resources to start a regular radio program on the topic of digital rights or internet shutdown circumvention (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

5.6.2 Continuous Development and Updating of Circumvention Tools

As mentioned, some technological solutions can indeed mitigate the negative impact of internet shutdowns in certain cases. However, experts and journalists have pointed out their shortcomings in terms of usability. As Abdullah notes, "some of the tools are not actually updated or they're not actually working (S. M. Abdullah, personal communication, May 6, 2024)." Therefore, journalists and advocates encourage technologists to continue developing these solutions, improving their functionalities, and continuously updating the tools according to changes in the legal environment or technological advancements. There is also room for tech communities and non-profit organisations to create new tools that serve different purposes than existing ones.

For example, J1_Cameroonian journalist mentioned a local tech community member who developed a tool for distributing news via SMS without the internet (J1_Cameroonian TV journalist, personal communication, May 27, 2024). However, the tool was prohibitively expensive due to SMS fees. Despite this, with financial and technical assistance from the international community, this tool has the potential to evolve into a more universal application.

5.6.3 The Importance of Local Engagement and Avoiding a Top-Down Approach

Abdullah observed that international communities are well-connected globally but are "not doing enough to connect with grassroots", and sometimes offer assistance with a top-down approach (S. M. Abdullah, personal communication, May 6, 2024). A lot of the popular tools in the market currently are developed by Western communities, leading to a gap between developers and user communities in terms of needs, user feedback, and usability. Developers are suggested to connect and engage with local journalists and civil society to introduce their tools to regions experiencing shutdowns. For example, from the interviews, it became apparent that journalists in shutdown areas could potentially benefit from certain tools but are unaware of them.

> “And some of the things that Bridgefy and Briar [offline messaging applications] are not actively promoting their tools in our kind of country… But mesh network is very important to circumvent complete internet shutdown or throttling. So this is very important, but they need to update their interface and need to improve their advocacy too” (S. M. Abdullah, personal communication, May 6, 2024).

Another consideration is that political contexts and citizens' tech literacy vary from country to country, as illustrated above. Therefore, it is essential for developers and human rights organisations to communicate with locals to determine what works for a particular country and what does not. For example, the founder of Briar discovered that some users gave up on using the application after a trial:

> “However, we see that the number of users rises quickly and then gradually drops off over time, which suggests that some of those people aren't finding the app as useful as they hoped - or it has other downsides, such as battery and mobile data usage, that cause them to stop using it. We need to do more research into why people start using the app and why they stop so that we can understand this pattern” (M. Rogers, email communication, May 27, 2024).

> “It is important to connect with local users and collect feedback from them to better understand their needs and the difficulties they face while using the application. As Anthonio stated, it's important to “listen to the users, to the people, to the local community” as the goal is “to provide solutions to them, and they are the ones

experiencing the shutdown" (F. Anthonio, #KeepItOn Campaign Manager, personal communication, May 2, 2024).

However, Rogers, the founder of Briar, pointed out limitations and obstacles in collecting user feedback. First, the technology communities often "lack the language skills and cultural knowledge to promote the app" in countries where it could be useful (email communication, May 27, 2024).

Another obstacle is that, developers like Briar may refrain from collecting user feedback due to privacy concerns. Rogers noted that "privacy-conscious users would be discouraged from using the app if it collected such data, despite its potential usefulness for app development" (M. Rogers, email communication, May 27, 2024).

One possible efficient way to bridge the language gap, and to increase trust to handle users' privacy concerns, is to have a local person or organisation acting as the connection point between external communities and the locals, whether someone from the diaspora or a local proficient in English. This person can act as the bridge to collect honest opinions and provide local insight, while making sure the person who local users talk to is trustworthy.

5.6.4 Providing Financial Support for Local Journalists in Shutdown Areas

Financial support is crucial, as mentioned by journalists interviewed, to holistically support journalists in shutdown areas, by helping journalists efficiently implement technological fixes or combat shutdowns in non-technological ways (J2_Kashmiri freelance journalist, personal communication, May 30, 2024). Despite some free open-source tools, certain circumvention tools are not free and can be expensive for countries with lower living standards. For example, both Abdullah and an Iranian independent journalist point out that international SIM cards are not popular in their countries due to their expense (J1_Iranian independent journalist, personal communication, March 14, 2024; S. M. Abdullah, personal communication, May 6, 2024). A Cameroonian TV journalist mentioned that he had tried an SMS-based news distribution system but had to discontinue it after a month due to high costs (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

At the moment, some interviewees express that there are not enough funding opportunities or donor attention in the field of shutdown circumvention. One possible

solution to this problem is for international non-profit organisations to provide financial support to journalists in shutdown regions, such as supplying them with smartphones with better specifications or purchasing VPNs and SIM cards for them. For example, donors or human rights organisations can subsidize journalists to purchase VPNs, cover their SMS costs, or cover the extra manpower costs they need during shutdowns. Or they can provide non-monetary resources, such as supplying them with smartphones with better specifications. This can allow journalists to make use of the technologies without budget concerns.

> "Because carrying out all these things is not easy. You have to give stipends to those who are working and also the material that you use" (J1_Cameroonian TV journalist, personal communication, May 27, 2024).

As mentioned before, connecting with local organisations to bridge the gap could improve the shortcomings, but sometimes it requires monetary incentives as it will occupy their working hours (S. M. Abdullah, personal communication, May 6, 2024). If funding could be provided in this regard, it could possibly help bridge the gap between locals and international communities.

5.6.5 Reviewing Methods for Categorising Internet Shutdowns

As mentioned earlier, the method by which governments shut down the internet is a critical factor in determining which circumvention tactics or technologies will be effective. However, currently, most digital rights organisations do not categorize internet shutdowns based on the method used. The #KeepItOn Shutdown Tracker Optimization Project (STOP), created and maintained by Access Now, is a systematic database that documents and contextualizes internet shutdown cases worldwide since 2016 (Access Now, 2024b). They categorize shutdowns as full shutdowns, bandwidth throttling, service-based blocking, and mobile and/or broadband network blocking. This method does not directly indicate how governments shut down the internet, making it difficult for circumvention researchers to gather precise data.

Abdullah also highlights a shortcoming within the tech community where measurement efforts often focus on the number of occurrences while neglecting duration, which is crucial for determining suitable circumvention tactics (personal communication, May 6, 2024).

> “But they count every type of internet shutdown as one… whether it lasts for three minutes, five hours, or just one day, it's counted as one shutdown” (S. M. Abdullah, personal communication, May 6, 2024).

5.6 Constraints in Circumventing internet Shutdowns

Despite the continuous efforts to mitigate the impact of internet shutdowns from both journalists and non-profit organisations, several constraints hinder the development and implementation of effective circumvention methods. This section highlights the technical and financial challenges in addressing internet shutdowns.

5.6.1 Difficulties in Developing Circumvention Tools

Developing circumvention tools remains challenging due to their technical nature. Rogers, highlighted that:

> “The basic issue is that internet and telephone infrastructure everywhere in the world is under political control, like any other infrastructure. Alternative means of communication over long distances, such as radio, are held under tight control as well… but we can't expect those [circumvention tools] to function as a replacement for internet and telephone” (M. Rogers, email communication, May 27, 2024).

Another challenge in developing circumvention tools is privacy concerns. Almost all interviewees mentioned surveillance measures imposed by their government. In countries where the government imposes internet shutdowns, digital rights are often severely restricted, making encrypted communication crucial to avoid legal risks. However, alternative means of communication that do not rely on internet can make it very hard to implement end-to-end encryption, or other secure and private communication system. Rogers said that the Briar team often has to “make trade-offs between connectivity and privacy,” and they prioritize privacy as their target users are at high risk of surveillance and repression (M. Rogers, email communication, May 27, 2024).

The limitations of users’ hardware also add difficulties in developing circumvention tools. For example, Apple’s iOS software ecosystem is often described as “closed” or “semi-closed,” as the products are tightly controlled devices, despite their high usability. Apple has complete control over the operating system, the applications that can be listed on the App Store, and the device hardware itself (Goldsmith, 2014). In simple terms, there are numerous

constraints when developing applications for iPhones. Rogers mentioned that while developing Briar, implementing peer-to-peer (P2P) functionality on iOS is not possible "due to restrictions on the things that apps are allowed to do while running in the background" (M. Rogers, email communication, May 27, 2024).

5.6.2 The High Financial Cost of Combatting Shutdowns

As suggested by interviewees, financial support is as important. However, this approach is constrained by government monitoring of financial transactions. In authoritarian countries, governments often monitor the bank transactions of politically sensitive individuals, such as high-profile journalists, to prevent them from receiving funds from international communities.

> "I recently received a grant from an organisation called Digital Rights Defenders…but they could not send the money to India because they were afraid of coming under scrutiny by the government" (J1_Kashmiri online news journalist, personal communication, May 23, 2024).

Sometimes, these limitations are not imposed by the country's authorities but are rather due to international relations, such as sanctions.

> "We are not connected to the international banking system. We are cut off. We are sanctioned by the US. Since all banking systems are cut off through SWIFT, which is an American-based service, we cannot connect to the international banking system" (J1_Iranian independent journalist, personal communication, March 14, 2024).

6. Limitation

One of the most significant limitations of this research is the selection of interviewees. First, the small sample size of three experts and eight journalists may not fully capture the diversity of experiences and perspectives across different regions and types of internet shutdowns. Not all countries that experienced shutdowns are covered, and not all formats of news are represented in each country. Secondly, there were a few limitations regarding the snowball sampling method. As recruitment messages were sent in English, only those proficient in English or those who knew someone who could translate were able to participate. As a result, selection bias is possible as the participants may have characteristics

that do not reflect the broader population of journalists. The purposive sampling method also carries a risk of researcher bias. Additionally, some technologists or experts did not respond to interview requests or were unavailable due to time constraints, leading to their exclusion from the study.

Another limitation concerns the content of the interviews. For most interviewees, English is not their first language, which could affect the quality of the data collected, potentially leading to misinterpretations or loss of nuanced information. Moreover, participants' security concerns might have led them to withhold sensitive information, affecting the comprehensiveness and holism of the discussion.

Qualitative research is inherently subjective as it relies on researchers' interpretation of data. During the process of coding and content analysis, different researchers might interpret the same data differently, leading to potential bias (Creswell & Poth, 2018). Content analysis can also potentially lack depth in understanding the context or meaning behind the data (Krippendorff, 2019). For example, technical backgrounds or political contexts might be missed during the coding and categorization of transcripts, leading to inaccuracy of interpretation of the data.

Furthermore, the researcher's language limitations pose another constraint. The researcher can only understand English, which may have restricted the background research, literature review, or selection of experts. Consequently, relevant information, research, or tools available in other languages might have been overlooked. However, this limitation should not be that significant as Access Now, a key source for this research, has connections with global organizations, providing a broader perspective.

These limitations should be considered when interpreting the findings of the study and in the context of developing strategies to support journalism during internet shutdowns in the future.

Conclusion and Discussion

Human rights and digital rights defenders have been seeking methods to help journalists mitigate the negative impacts of internet shutdowns since authorities began using this tactic to silence journalists and oppress freedom of expression. Over the years, researchers and scholars have examined this issue while primarily exploring and documenting the patterns,

triggers, and impacts of shutdowns. Some previous research has also looked into ways to circumvent internet shutdowns.

This research focuses more narrowly on what journalists specifically can do to cope with internet shutdowns. Addressing the research questions, journalists have been innovating various circumvention tactics to maintain reporting during internet shutdowns, including collaborating with different communities, developing contingency protocols, and making use of different tools or applications to document news material or maintain a certain level of communication.

It is challenging to define "the best way" to cope with internet shutdowns, as there is no one-size-fits-all solution. When seeking ways to cope with an internet shutdown, journalists should consider multiple factors: how the authorities shut down the internet, each individual's threat model and the risks they face, the potential legal consequences, and their willingness to bear these risks to find workable solutions, as these factors vary from country to country, and even city to city.

This raises a fundamental issue in the current research field of internet shutdowns: the methods for categorising internet shutdowns must evolve so that circumvention researchers can more effectively find solutions.

The literature review shows that researchers and scholars have addressed the topic of internet shutdown circumvention, and most findings from this research echo the empirical studies. However, there are some new findings in this research: specifically the importance of working with diaspora communities and the use of satellite internet. One reason these solutions have not been mentioned much before is that they are relatively new; emerging as technology develops and economic situations change over the past years.

Despite the hard work of researchers, journalists, and digital rights communities, internet shutdowns are, unfortunately still an expanding phenomenon and are worsening every year. More authorities from different continents are imposing shutdowns, and these shutdowns are getting longer. Does this mean all the empirical research and advocacy work is useless? Various factors contribute to the increase in internet shutdowns. One obvious cause is the increasing oppressiveness by governments targeting media, meaning the collective effort from advocates, technologists and journalists, among others, cannot keep up.

During the research, one common theme mentioned was the struggle to circumvent a full shutdown, which remains one of the biggest unsolved problems. Other factors include the gap between human rights communities and on-the-ground journalists, an interesting observation from this research. While there seem to be many circumvention tools available and various parties working on circumvention, journalists do not appear to suffer less from shutdowns. This research highlights some shortcomings in current digital rights efforts, such as the lack of communication with local communities and the struggle between privacy and the efficiency of tools. This gap leads to situations where journalists have never heard of potentially useful tools, meaning that even if useful tools are developed, they may not reach those who need them. Particularly, some interviewees in this research work at major news outlets in their countries and should be among the first to receive information from international communities.

Fighting against internet shutdowns is a collective effort involving academic researchers to explore the broader picture, advocates to address the problem in the long run, technologists to develop temporary circumvention solutions, and journalists striving to maintain their work. The international communities should enhance their work with local communities, provide better training, conduct more comprehensive research, and offer local journalists a broader range of support and resources.

That being said, internet shutdown circumvention research is and should be a continuous effort, as technology - both for circumvention and to oppress press freedom - is ever-changing, along with the political context. Future research could include a larger sample size, taking into consideration journalists' nationalities, positions, the format of news, gender, etc., in order to achieve more holistic insights to ultimately protect the freedom of the press and expression.

Summary

Internet shutdowns have increasingly become a tactic employed by governments worldwide to restrict press freedom. This research aims to investigate potential and existing efficient methods for maintaining journalism during internet shutdowns, based on in-depth interviews with three experts and eight journalists from regions affected by shutdowns. The results show that common challenges journalists face during shutdowns include difficulties in communicating with different parties, and increased government oppression. The findings highlight several technological solutions, such as the use of different tools, as well as the potential of satellite technology as an alternative source of internet. Regarding non-technological circumvention, journalists emphasized the importance of maintaining a network within both locally and internationally, as well as setting up contingency plans in advance. Given the difficulties in circumventing a full shutdown, journalists stressed the importance of recording and archiving news events. There is no one-size-fits-all solution to shutdowns; effective strategies depend on various factors such as the scale and local laws regarding certain technologies. The international communities is encouraged to engage with locals, and to continue developing circumvention tools to address the ever-changing political and technical landscape. Methods for categorizing internet shutdowns should also be reviewed to more effectively identify solutions.

Vypínání internetu se stále častěji stává taktikou, kterou vlády po celém světě používají k omezování svobody tisku. Cílem tohoto výzkumu je na základě hloubkových rozhovorů se třemi odborníky a osmi novináři z regionů postižených výpadky internetu, prozkoumat možné a existující účinné metody pro zachování chodu kvalitní žurnalistiky během výpadků. Výsledky ukazují, že mezi běžné problémy, kterým novináři během výpadků čelí, patří obtíže při komunikaci s různými stranami a zvýšený útlak ze strany vlády. Zjištění poukazují na několik technologických řešení, jako je používání různých nástrojů, a také na potenciál satelitní technologie jako alternativního zdroje internetu. Co se týče netechnologického obcházení, novináři zdůraznili důležitost udržování sítě kontaktů lokálních i mezinárodních, stejně jako vytváření krizových plánů v předstihu. Vzhledem k obtížím při obcházení úplného vypnutí internetu, novináři zdůraznili význam nahrávání a archivace zpravodajskýchp událostí. Neexistuje žádné univerzální řešení vypnutí; účinné strategie závisí na různých faktorech, jako je rozsah a místní zákony týkající se určitých technologií. Mezinárodní komunity se vyzývají, aby spolupracovaly s místními obyvateli a pokračovaly ve vývoji nástrojů pro obcházení, které by reagovaly na neustále se měnící politické a

technické podmínky. Měly by se také přezkoumat metody kategorizace vypínání internetu, aby bylo možné účinněji určit řešení.

List of References

Access Now. (2020, February). Targeted, cut off, and left in the dark. https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

Access Now. (2020). No more internet shutdowns! Let's #KeepItOn. Retrieved February 22, 2023, from https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/

Access Now. (2022, June 3). Internet shutdown types and taxonomy: Tech behind network interference. Access Now. https://www.accessnow.org/publication/internet-shutdown-types/

Access Now. (2024a, May 15). Tracking internet shutdowns: Our STOP methodology. Access Now. https://www.accessnow.org/guide/shutdown-tracker-optimization-project/

Access Now. (2024b). The Shutdown Tracker Optimization Project (STOP) dataset. https://www.accessnow.org/keepiton-data

Activate Rights. (n.d.). Who are we. *Activate Rights*. Retrieved June 28, 2024, from https://activaterights.org/who-are-we/

Albrecht, M. R., Blasco, J., Jensen, R. B., & Mareková, L. (2021). Mesh messaging in large-scale protests: Breaking bridgefy. In K. G. Paterson (Ed.), *Topics in Cryptology – CT-RSA 2021* (pp. 375–398). Springer International Publishing. https://doi.org/10.1007/978-3-030-75539-3_16

Amnesty International. (2016, March 23). Egypt: Unprecedented crackdown on NGOs. *Amnesty International*. https://www.amnesty.org/en/latest/press-release/2016/03/egypt-unprecedented-crackdown-on-ngos/

Anderson, C. (2012). The hidden internet of Iran: Private address allocations on a national network. *arXiv*. https://doi.org/10.48550/ARXIV.1209.6398

Arthur, C. (2011, January 28). Egypt cuts off internet access. *The Guardian*. https://www.theguardian.com/technology/2011/jan/28/egypt-cuts-off-internet-access

Ayalew, Y. E. (2019). The internet shutdown muzzle(s) freedom of expression in Ethiopia: Competing narratives. *Information & Communications Technology Law, 28*(2), 208–224. https://doi.org/10.1080/13600834.2019.1619906

Balkin, J. M. (2003). Digital speech and democratic culture: A theory of freedom of expression for the information society. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.470842

Beh Lih Yi. (2021, February 25). Myanmar's internet shutdown: What you need to know. *News.Trust.Org*. https://news.trust.org/item/20210217141412-ljfpg/

Bhalla, N. (2021, November 5). SIMs to leaflets: Sudanese find ways to skirt net outage. *Thomson Reuters Foundation News*. https://news.trust.org/item/20211104180126-c7sd0/

Bhatia, K. V., Elhussein, M., Kreimer, B., & Snapp, T. (2023). Protests, internet shutdowns, and disinformation in a transitioning state. *Media, Culture & Society, 45*(6), 1101–1118. https://doi.org/10.1177/01634437231155568

Biernacki, P., & Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological Methods & Research, 10*(2), 141–163. https://doi.org/10.1177/004912418101000205

Bischof, Z. S., Pitcher, K., Carisimo, E., Meng, A., Bezerra Nunes, R., Padmanabhan, R., Roberts, M. E., Snoeren, A. C., & Dainotti, A. (2023). Destination unreachable: Characterizing internet outages and shutdowns. *Proceedings of the ACM SIGCOMM 2023 Conference* (pp. 608–621). https://doi.org/10.1145/3603269.3604883

Bivens, R. K. (2008). The internet, mobile phones and blogging: How new media are transforming traditional journalism. *Journalism Practice, 2*(1), 113–129. https://doi.org/10.1080/17512780701768568

Björksten, G. (2022). A taxonomy of internet shutdowns: The technologies behind network interference. Access Now.

Briar. (2021, June 7). Briar 1.3 released - Image attachments, profile images and disappearing messages. *Briar*. https://briarproject.org/news/2021-briar-1.3-released/

Briar. (n.d.). How it works. *Briar*. Retrieved June 28, 2024, from https://briarproject.org/how-it-works/

Cambridge University Press. (n.d.). Internet. In *Cambridge English Dictionary*. Retrieved June 25, 2024, from https://dictionary.cambridge.org/dictionary/english/internet

Carlson, M. (2016). Metajournalistic discourse and the meanings of journalism: Definitional control, boundary work, and legitimation. *Communication Theory, 26*(4), 349-368. https://doi.org/10.1111/comt.12088

Chandra, Y., & Shang, L. (2019). *Qualitative research using R: A systematic approach*. Springer Nature Singapore. https://doi.org/10.1007/978-981-13-3170-1

Chari, T. (2024). Digital authoritarianism and epistemic rights in the global south: Unpacking internet shutdowns in Zimbabwe. In M. Aslama Horowitz, H. Nieminen, K. Lehtisaari, & A. D'Arma (Eds.), *Epistemic rights in the era of digital disruption* (pp. 139–153). Springer International Publishing. https://doi.org/10.1007/978-3-031-45976-4_10

Chatterjee, S. (2019). Exploring possible solutions to curb internet shutdowns in India. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3644879

Cloudflare. (n.d.). What is DNS? *Cloudflare*. Retrieved June 23, 2024, from https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/

Collins, K. (2019, October 31). Inside the dystopian nightmare of an internet shutdown. *CNET*. https://www.cnet.com/tech/services-and-software/features/inside-the-dystopian-nightmare-of-an-internet-shutdown/

Comer, D. E. (2018). *The internet book* (5th ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9780429447358

Committee to Protect Journalists. (2021, April 13). Digital Safety: Internet shutdowns. *Committee to Protect Journalists*. https://cpj.org/2021/04/digital-safety-internet-shutdowns/

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Sage Publications, Inc.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications, Inc.

Dahlberg-Grundberg, M. (2016). Technology as movement: On hybrid organizational types and the mutual constitution of movement identity and technological infrastructure in digital activism. *Convergence: The International Journal of Research into New Media Technologies, 22*(5), 524–542. https://doi.org/10.1177/1354856515577921

Danao, M. (2023, October 16). Are VPNs legal? The worldwide guide. *Forbes*. https://www.forbes.com/advisor/in/business/are-vpns-legal/

DiBona, C., Ockman, S., & Stone, M. (1999). *Open sources: Voices from the open source revolution*. O'Reilly Media.

Dobrev, D. (2016). *Wireless mesh networks: Architectures and protocols*. Springer.

Faboade, D. (2024, May 20). Starlink emerges as Nigeria's third-largest internet service operator in Q4 2023. *Space in Africa*. https://spaceinafrica.com/2024/05/20/starlink-emerges-as-nigerias-third-largest-isp-in-q4-2023/

Feldstein, S. (2021). *The rise of digital repression: How technology is reshaping power, politics, and resistance* (1st ed.). Oxford University Press. https://doi.org/10.1093/oso/9780190057497.001.0001

Ferguson, P., & Huston, G. (1998, October). What is a VPN? In *Proceedings of the OPENSIG'98 Workshop on Open Signalling for ATM, Internet and Mobile Networks*. Toronto, Canada.

Foros, Ø., & Hansen, B. (2001). Competition and compatibility among internet service providers. *Information Economics and Policy, 13*(4), 411–425. https://doi.org/10.1016/s0167-6245(01)00044-0

Fuchs, C. (2007). *Internet and society*. Routledge. https://doi.org/10.4324/9780203937778

Garbe, L. (2023). Pulling through elections by pulling the plug: Internet disruptions and electoral violence in Uganda. *Journal of Peace Research*. https://doi.org/10.1177/00223433231168190

Goldsmith, A. (2005). *Wireless communications*. Cambridge University Press.

Goldsmith, B. (2014). The smartphone app economy and app ecosystems. In G. Goggin, & L. Hjorth (Eds.), *The Routledge companion to mobile media* (pp. 171-180). Routledge.

Goleniewski, L., & Jarrett, K. (2007). *Telecommunications essentials: The complete global source* (2nd ed.). Addison-Wesley.

Grinko, M., Qalandar, S., Randall, D., & Wulf, V. (2022). Nationalizing the internet to break a protest movement: Internet shutdown and counter-appropriation in Iran of late 2019. *Proceedings of the ACM on Human-Computer Interaction, 6*(CSCW2), 1–21. https://doi.org/10.1145/3555205

Grover, R. (2023). Contingent connectivity: Internet shutdowns and the infrastructural precarity of digital citizenship. *New Media & Society*. https://doi.org/10.1177/14614448231176552

Grush, L. (2020, October 27). SpaceX begins public beta testing of Starlink constellation at $99 a month. *The Verge*. https://www.theverge.com/2020/10/27/21536073/spacex-starlink-public-beta-testing-email-user-terminal

Horizontal. (n.d.). Work—Horizontal. *Horizontal*. Retrieved July 22, 2024, from https://wearehorizontal.org/our-work

Internews. (2023, February 1). Home - Prepare prevent resist. *OPTIMA*. https://preparepreventresist.org/

Jones, S. (2019, March 13). Venezuela blackout: What caused it and what happens next? *The Guardian*. https://www.theguardian.com/world/2019/mar/13/venezuela-blackout-what-caused-it-and-what-happens-next

Kaplan, E. D., & Hegarty, C. J. (2006). *Understanding GPS: Principles and applications* (2nd ed.). Artech House.

Kaufman, C., Perlman, R., & Speciner, M. (2016). *Network security: Private communication in a public world* (2nd ed.). Prentice Hall.

Keary, T. (2024, April 30). What is a proxy server? *Forbes*. https://www.forbes.com/advisor/business/what-is-a-proxy-server/

Klitgaard, T. (n.d.). About. *Good Tape*. Retrieved June 26, 2024, from https://goodtape.io/about/

Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications, Inc. https://doi.org/10.4135/9781071878781

Lee, J. (2009). Global positioning/gps. In *International Encyclopedia of Human Geography* (pp. 548–555). Elsevier. http://dx.doi.org/10.1016/b978-008044910-4.00035-3

Linow, O., & Freund, A. (2022, March 7). How to send messages without the internet. *Deutsche Welle*. https://www.dw.com/en/how-to-send-messages-in-ukraine-if-the-internet-shuts-down/a-61041676

Madenga, F. (2021). From transparency to opacity: Storytelling in Zimbabwe under state surveillance and the internet shutdown. *Information, Communication & Society, 24*(3), 400–421. https://doi.org/10.1080/1369118X.2020.1836248

Maini, A. K., & Agrawal, V. (2007). *Satellite technology: Principles and applications*. John Wiley & Sons.

Malan, D. (2017). Internet - CS50's understanding technology 2017 [Video]. In *Harvard School of Engineering and Applied Sciences*. https://www.youtube.com/watch?v=n_KghQP86Sw

Marchant, E. (2020). A spectrum of shutdowns: Reframing internet shutdowns from Africa.

Mare, A. (2020). State-ordered internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication, 14*, 4244–4263.

Mason, J. (2002). *Qualitative researching* (2nd ed.). Sage Publications Ltd.

Meiklejohn, A. (1965). *Political freedom: The constitutional powers of the people*. Oxford University Press.

Merrill, J. C. (1994). *Legacy of wisdom: Great thinkers and journalism* (1st ed.). Iowa State University Press.

Miculan, M., & Vitacolonna, N. (2023). Automated verification of Telegram's MTProto 2.0 in the symbolic model. *Computers & Security*, *126*, 103072. https://doi.org/10.1016/j.cose.2022.103072

Miller, G. (2023, October 26). Finding you: The network effect of telecommunications vulnerabilities for location disclosure. *The Citizen Lab*. https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/#roaming-sims-and-services-101

Moinuddin, S. (2021). Spatial mapping of digital shutdown in India. In S. Moinuddin, *Digital shutdowns and social media* (pp. 149–164). Springer International Publishing. https://doi.org/10.1007/978-3-030-67888-3_7

Ngangum, P. T. (2023). Internet shutdowns in semi-authoritarian regimes. In I. Nordenstreng, & F. Nkwi (Eds.), *Communication rights in Africa* (pp. 165–182). Routledge. https://doi.org/10.4324/9781003388289-13

Opensource.com. (n.d.). *What is open source?* Opensource.Com. Retrieved July 30, 2024, from https://opensource.com/resources/what-open-source

O'Neill, A., Tatham, R., Carter, S., Tsirtsis, G., & Dann, A. (1998). An overview of internet protocols. *BT Technology Journal, 16*(1), 126–139. https://doi.org/10.1023/A:1009684924606

Oram, A. (2001). *Peer-to-peer: Harnessing the benefits of a disruptive technology*. O'Reilly Media.

Pandow, B. A. (2020). "The idea is to kill journalism": Kashmiri journalists on what it's like working under lockdown, an internet blackout and a new draconian media law. *Index on Censorship, 49*(3), 17–19. https://doi.org/10.1177/0306422020958271

Peeters, C., Patton, C., Munyaka, I. N. S., Olszewski, D., Shrimpton, T., & Traynor, P. (2022). Sms otp security (Sos): Hardening sms-based two factor authentication. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (pp. 2–16). https://doi.org/10.1145/3488932.3497756

Richey, S., & Taylor, J. B. (2018). *Google and democracy: Politics and the power of the internet*. Routledge is an imprint of the Taylor & Francis Group, an Informa Business.

Rosson, Z., Tackett, C., Anthonio, F., & Access Now. (2023). Weapons of control, shields of impunity: Internet shutdowns in 2022. Access Now. Retrieved from https://www.accessnow.org/keepiton-2022-report

Rosson, Z., Tackett, C., Anthonio, F., & Access Now. (2024). Shrinking democracy, growing violence: Internet shutdowns in 2023. Access Now. Retrieved from https://www.accessnow.org/keepiton-2023-report

Rydzak, J., Karanja, M., & Opiyo, N. (2020). Dissent does not die in darkness: Network shutdowns and collective action in African countries. *International Journal of Communication, 14*.

Ryng, J., Guicherd, G., Saman, J. A., Choudhury, P., & Kellett, A. (2022). Internet shutdowns. *The RUSI Journal, 167*(4–5), 50–63. https://doi.org/10.1080/03071847.2022.2156234

Satriawan, I., Elven, T. M. A., & Lailam, T. (2023). Internet shutdown in Indonesia: An appropriate response or a threat to human rights? *Sriwijaya Law Review, 7*(1), 19. https://doi.org/10.28946/slrev.Vol7.Iss1.1018.pp19-46

Selnes, F. N. (2020). Internet restrictions in Uganda: Examining their impact on journalism. *Information, Communication & Society, 24*(3), 490–506. https://doi.org/10.1080/1369118X.2020.1859580

Shachtman, N. (2012, November 29). Syria has just been taken offline. *WIRED*. https://www.wired.com/2012/11/syria-offline/

Shah, N. (2021). (Dis)information blackouts: Politics and practices of internet shutdowns.

Shinder, L., & Cross, M. (2008). iPod, Cell Phone, PDA, and BlackBerry Forensics. In *Scene of the Cybercrime* (pp. 347–379). Elsevier. http://dx.doi.org/10.1016/b978-1-59749-276-8.00008-x

Shuler, R. (2020, September). How does the internet work? [Online]. *Stanford University*. https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm

Sinaiee, M. (2024, April 1). Government-approved hike in cost of internet angers Iranians. *Iran International*. https://www.iranintl.com/en/202401037934

SMSWithoutBorders. (2023, February 7). SmsWithoutBorders (SWOB). *Afkanerd*. https://afkanerd.github.io/blog/swob/

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Taye, B., & Access Now. (2019, July). The state of internet shutdowns around the world: The 2018 #KeepItOn Report. Retrieved from https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf

Tella. (n.d.). Tella features. *Tella*. Retrieved July 6, 2024, from https://tella-app.org/features

Townsend, M. (2024, May 16). Starlink internet shutdown in Sudan will punish millions, Elon Musk warned. *The Guardian*. https://www.theguardian.com/global-development/article/2024/may/16/starlink-internet-shutdown-in-sudan-will-punish-millions-elon-musk-warned

Truscello, M. (2023). The internet shutdown and revolutionary politics: Defining the infrastructural power of the internet. *South Atlantic Quarterly, 122*(4), 811–826. https://doi.org/10.1215/00382876-10747811

Tsandzana, D. (2023). Cabo Delgado também é Moçambique. In I. Nordenstreng, & F. Nkwi (Eds.), *Communication rights in Africa* (pp. 91–109). Routledge. https://doi.org/10.4324/9781003388289-8

Vargas-Leon, P. (2016). Tracking internet shutdown practices: Democracies and hybrid regimes. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in internet governance* (pp. 167–188). Palgrave Macmillan US. https://doi.org/10.1057/9781137483591_9

Wagner, B. (2018). Authoritarian practices in the digital age: Understanding internet shutdowns: A case study from Pakistan. *International Journal of Communication, 12*, 22.

List of Appendices

Appendix no. 1: Glossary (table)

Appendix no. 2: Expert Interviewee Information and Specialties (table)

Appendix no. 3: Semi-structured interview-guide (list)

Appendix 1: Glossary

Term	Definition
BGP	Border Gateway Protocol, the protocol that enables data routing across the internet. (O'Neill et al., 1998)
Cellular network	A wireless digital/radio network made up of cells served by transceivers called base stations, providing extensive coverage and seamless connectivity for mobile devices (Shinder & Cross, 2008; Goldsmith, 2005).
Cloudflare	An American company providing content delivery network services, cloud cybersecurity, DDoS mitigation, Domain Name Service, among other services to enhance the performance, security, and reliability of websites. (Cloudfare, n.d.)
DNS	Domain Name Servers, responsible for translating domain names into IP addresses.
Encryption	The process of converting data into a code to prevent unauthorized access, ensuring that the information is only accessible to those who have the decryption key (Stallings, 2017).
End-to-end encryption	A type of encryption where data is encrypted on the sender's device and can only be decrypted on the recipient's device, ensuring no intermediaries can access the data.
GPS	Global Positioning System, a satellite-based navigation system providing location and time information. (Lee, 2009)
GPS spoofing	The act of deceiving a GPS receiver by broadcasting fake GPS signals, thereby manipulating the receiver's location data (Kaplan & Hegarty, 2006).

IP address	Internet Protocol address, a unique identifier assigned to each device connected to a network.
Internews	A media support nonprofit working in over 100 countries to promote free and independent media.
Landline	Refers to voice and data communications transmitted through physical cables as opposed to wireless communications, including fixed telephony and wired data services (Goleniewski & Jarrett, 2007).
Mesh Network	A network topology where each node (device) is interconnected, allowing devices to rely on wireless technologies such as Bluetooth Low Energy (BLE) to create communication networks without internet connectivity (Albrecht et al., 2021; Dobrev, 2016).
MTProto	Mobile Transport Protocol, a suite of security protocols for instant messaging at the core of the Telegram messenger application (Miculan & Vitacolonna, 2023).
OONI	Open Observatory of Network Interference, a global community project measuring internet censorship around the world.
Packets	Data divided into small units and transmitted over a network along with metadata for routing.
Peer-to-peer (P2P)	A decentralized network architecture where each participant (peer) can act as both a client and a server, sharing resources directly with other peers without needing a central coordinator (Oram, 2001).
Proxy	Proxy servers are systems or applications that act as a gateway between a client and web servers on the internet, providing an intermediary to add security and mask the user's IP address (Keary, 2024).
VPN	Virtual Private Network, a service that encrypts internet connections and masks IP addresses to provide privacy and security online.

Open source	Software for which the original source code is made freely available and may be redistributed and modified according to the user's requirements, promoting collaborative development and transparency. (Opensource.com, n.d)
SMS	Short Message Service

Appendix 2: Expert Interviewee Information and Specialties

Interviewee	Position and Affiliation	Specialties and Covered Topics During the Interviews
Felicia Anthonio	The #KeepItOn Campaign Manager at Access Now, a global campaign fighting against internet shutdowns worldwide (Access Now, 2024).	- General information about internet shutdowns - Prediction of trends in internet shutdowns - Experience, skills, and obstacles in anti-internet Shutdown advocacy - Observations, reflections, and advice on working with technologists
Shoeb Md Abdullah	Founder of Activate Rights, a voluntary initiative focused on internet freedom and the anti-shutdown movement in Bangladesh (Activate Rights, n.d.). Network Measurement Fellow in OPTIMA Project, Internews' program that supports collaboratively developed resources to enable better responses to major instances of internet shutdowns in Africa (Internews, 2023).	- Available tools and countermeasures for internet shutdowns - Experience, skills, and obstacles in shutdown circumvention training and advocacy - Opinion and advice for international communities

Michael Rogers	Founder of Briar project, a peer-to-peer encrypted messaging app with no internet access required (Briar, n.d.).	- Information and usage of peer-to-peer messenger tools - Promoting and educating journalists on shutdown circumvention tools - The technological side of internet shutdown and circumvention - Experience in developing shutdown circumvention tools as a technologist

Appendix 3: Semi-structured interview-guide

Technology experts (in interview order):

Michael Rogers (Founder of Offline Messager app Briar)

Shutdown:

1. Based on your understanding and experience, what are the most significant challenges journalists facing in shutdown areas?
2. What did technologists, advocates, and the international communities do wrong or not do enough to combat internet shutdowns in general?
3. How can the international community, including human rights advocates and technologists, bridge the gap and promote their technologies and ideas to the general public? And what do you think that they are not paying enough attention to? Share your experience and thoughts.
4. For you, what are the biggest obstacles to combating internet shutdowns?

Briar specific:

1) Story behind founding Briar.
2) Under what circumstances and situation should Briar be used?
3) How, and in what ways, did you anticipate that Briar should contribute to this combating internet shutdown?
4) Does the app achieve the initial goals?
5) Questions about User data:
   a) How many current users does Briar have?
   b) Where are they from?
   c) To which socio-economic groups or occupations do the users mainly belong?
   d) How frequently do they use the app?
   e) Have you received any user feedback? And what are they?
   f) How much do you interact with users? Why or why not?
   g) Any other information about the users that you know.
   h) Why do you think the user number is ideal/ not ideal?
   i) If you don't know the answer of any of the questions above, did you try to obtain the information but failed? If you did not try, why?

6) What improvements can Briar make to better cater to people's needs during internet shutdowns?
7) What are the biggest obstacles to getting people to use Briar?
8) How did (/will) you promote Briar?
9) In your opinion, has Briar been doing a good job at promoting globally? Why and why not?

Felicia Anthonio (**The #KeepItOn Campaign Manager at Access Now)**

Structured:

1. Based on your understanding and experience, what are the greatest challenges facing journalists in shutdown areas?
2. What did the international communities do wrong, or not do enough of, to combat internet shutdow
3. How can the international community, including human rights advocates and technologists, bridge the gap and promote their technologies and ideas to the general public? Share your experience.
4. For you, what are the biggest obstacles to combat internet shutdown?

Unstructured:

1) Describe the global trend of internet shutdowns.
2) What are the biggest difficulties people face when combating internet shutdowns? (e.g. financial factors, lack of technical knowledge)
3) Your Suggestion: Most effective approaches to combat internet shutdowns (e.g. technical and non-technical methods)
4) Your Observation: Approaches that are currently being used to combat internet shutdowns (e.g. technical and non-technical methods)
5) What are the biggest difficulties or obstacles people, especially journalists, face when combating shutdowns or implementing expert-developed solutions?
6) What are the most important actions that advocates, stakeholders, or the international community should take to bridge the gap?
7) Have you heard of Bridgefy, Briar, VPN, international SIM, Tella?
   a) Why do you think the apps do not have a larger user base and, therefore, do not effectively help local communities combat shutdowns, given the fact that people are still suffering a lot of shutdowns?
   b) How can the tool be utilised more effectively?

c) Possible questions pertaining to the statements made by the tech experts.

Shoeb Md Abdullah (Trainer)

Structured:

1. Based on your understanding and experience, what are the greatest challenges facing journalists in shutdown areas?
2. What did the international communities do wrong, or not do enough of, to combat internet shutdowns?
3. How can the international community, including human rights advocates and technologists, bridge the gap and promote their technologies and ideas to the general public? Share your experience.
4. For you, what are the biggest obstacles to combat internet shutdown?

Unstructured:

5. Tell me about the internet shutdowns in Bangladesh, such as pattern, frequency, occasion, how the government shut the internet down, and anything you think it's important or relevant.

6) Tell me more about your advocacy and advocacy training work.
   a) What exactly do you do?
   b) Who is your target audience?
   c) Who do you reach out to people you train?
   d) What do you teach them?
   e) Do you work with international organizations or communities? If you do, in what way?

7. What is your biggest challenge or obstacle carrying out your work?
8. Your Suggestion: Most effective approaches to combat internet shutdowns, both long-term and short-term. (e.g. technical and non-technical methods)
9. Your Observation: Approaches that are currently being used to combat internet shutdowns, both long-term and short-term. (e.g. technical and non-technical methods)
10. What are the biggest difficulties or obstacles people, especially journalists, face when combating shutdowns or implementing expert-developed solutions? (e.g. financial factors, lack of technical knowledge)
11. What are the most important actions that advocates, stakeholders, or the international community should take to bridge the gap?

12) According to my literature review, the following tools were mentioned. Have you heard of Bridgefy, Briar, VPN, international SIM, Tella?
    a) Why do you think the apps do not have a larger user base and, therefore, do not effectively help local communities combat shutdowns, given the fact that people are still suffering a lot of shutdowns?
    b) How can the tool be utilised more effectively?

Journalists:

Experience in internet shutdown

1. How long did the shutdown(s) last, and what was/ were the occasion(s)?
2. Were you informed before it happened? If so, did you do anything to prepare for it?
3. Do you think the authorities achieved what they wanted? For example, was it successful if they wanted to stop an uprising?
4. What was the biggest loss after the shutdown, economically or democratically?

Experience & Reflection for future occurrence of shutdown"

5) Descript your work during the shutdown periods
    a) What exactly do you do?
    b) Who is your target audience?
    c) Who did you have to contact for your reporting (e.g. interviewees, government representatives, editors). And how?
    d) How did you gather information, e.g., news, announcements, etc.?
    e) How did you publish?
6. What was the main challenge at work initially and later on?
7. What did citizens do to stay connected to what was happening?
8. What did journalists do wrong during the shutdown?
9. Looking back, what would you have done differently, or what would you change if the situation occurred again?
10. Your Observation: Approaches currently being used to combat internet shutdowns, both long-term and short-term. (e.g. technical and non-technical methods)
11. Do you see a lot of difficulties for the media and freedom of speech at the time? For example, was there more misinformation?

Views on existing technology and international communities

12. Did you use any of the following tools or workarounds? Share your thoughts and experiences. Bridgefy, Briar, VPN, international SIM, Tella.
13. If you have not, do they sound appealing to you in theory? Why or why not? How can it be improved?
14. What can technologists do to help? For example, is there any helpful technology or tool you wish was invented?
15. What can the international community do to help, both technologically and otherwise?