The Terminologies and Taxonomies of Internet Shutdowns

Michael Collyer
University of Oxford

Joss Wright
University of Oxford

Abstract

In this paper, we explore definitions and synonyms of an 'internet shutdown' and propose a non-technical framework for internet shutdown 'types', namely, the Four Pillars of Internet Shutdowns. We also collate existing taxonomies surrounding internet shutdowns or similar phenomena and propose a non-technical framework for grouping shutdowns. Both frameworks may be helpful for non-technical researchers looking to narrow the scope of their research on internet shutdowns in a methodologically principled manner. The key contribution of this paper is that it aims to provide a simplified approach to current terms and taxonomies of internet shutdowns, with an intended target audience of computational social scientists and policymakers. Our paper is novel, as it explores the grey areas between shutdown definitions and taxonomies and goes beyond the current "spectrum" approach to shutdowns.

1 Introduction

Internet shutdowns are an extreme form of internet censorship which has steadily increased since 2007 [12]. Despite their use as a tool for digital repression for over 15 years, there is uncertainty surrounding what an "internet shutdown" is and the types that exist. Additionally, existing taxonomies of shutdowns focus on the technical methods of implementation, as such, there is a gap for a taxonomy focused on non-technical measurements, such as duration and geographic scope. By reframing terminologies used when discussing shutdowns and creating a taxonomy based on temporal and geospatial variables, this paper provides two novel frameworks which could be helpful for a non-technical audience. This paper is structured in two parts, and will discuss shutdowns in the context of terminologies and then taxonomies.

Regarding terminologies, several organisations have proposed definitions of an internet shutdown, for example, Access Now, Internet Freedom India, the Digital Empowerment Foundation, the African School of Internet Governance (AfriSIG), and the African Network Information Centre (AFRINIC). Comparing and contrasting these definitions is the first step to clarifying the term "internet shutdown". Beyond these definitions, numerous synonyms or related terms exist, for example, blackout, kill switch, throttling, digital siege, or digital curfew. These terms, sometimes used interchangeably by academics, journalists, or civil society organisations, may contribute to the confusion about what is and is not an internet shutdown. Furthermore, the sheer number of terms that refer to a shutdown may explain why some studies often group all types of shutdowns as an "internet shutdown" rather than making a distinction between, for example, a "network shutdown" and "platform blockage". As such, there is merit in proposing a simplified framework. At the minimum, this paper provides a helpful overview of the variety of definitions of an "internet shutdown" and related terms.

Regarding taxonomies, several authors or organisations have proposed ways of classifying different types of internet shutdowns or outages [3, 19, 41, 43]. For the vast majority, these taxonomies are concerned with the technical reasons for how an internet shutdown occurred, for example, DNS or IP blocking. While there is value in comparing existing taxonomies, we believe that proposing a non-technical taxonomy would be the largest value add for non-technical researchers aiming to analyse shutdowns in a methodologically principled manner. At current, many studies group all forms of internet shutdowns into the same bucket. Therefore, there is value in differentiating between, for example, a large geographic and long-duration shutdown (Type 1A) from a small geographic and short-duration shutdown (Type 3C). Creating a matrix of shutdowns in this format ensures that similar types can be grouped and analysed within and between types.

For both the terminologies and taxonomies aspects of this paper, we acknowledge there are nuances and grey areas. Just as there are blurred lines between what is and what is not an internet shutdown, there are blurred lines between different types of shutdowns and how to group them. However, despite the overlapping nature of numerous concepts discussed below, we believe this paper is still valuable to academia, government and civil society and acts as a helpful guide.

We will first provide an overview of when "internet shutdowns" crept into the digital repression toolkit, its etymology, and how they are situated within the broader literature of internet censorship and information controls. We then provide an overview of terms related to internet shutdowns and posit a reframing of the terminological landscape. We then explore different taxonomies of internet shutdowns and suggest a new framework for classifying shutdowns based on non-technical descriptors (such as geographic scope or duration). Finally, we address the limitations of this paper and conclude with areas for future research.

2 History of "Internet Shutdowns"

2.1 Internet Shutdowns, Internet Censorship, and Information Controls

Internet shutdowns are a form of internet censorship, and internet censorship is a form of information control. A shutdown is a unique act of censorship. Not only given its relatively indiscriminate nature relative to, for example, content moderation, but also given the emergence of the use of the term "internet shutdown" and the uncertainties about its definition.

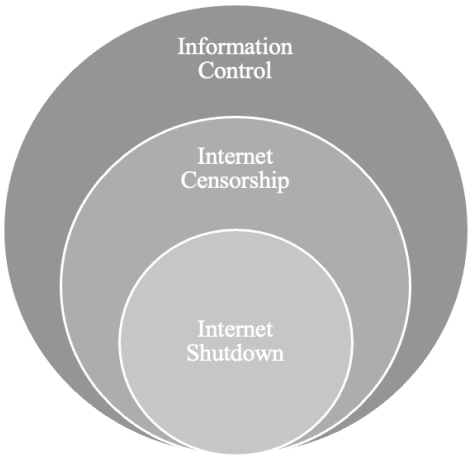

Figure 1: Internet Shutdowns within the Broader Literature

An internet shutdown is a type of information intervention that is usually driven by a State. Adopting Weber's definition of a State, we see that a State is a polity which has a monopoly on the 'legitimate use of violence' [17]. The aspect to emphasise here is legitimacy, as it is this legitimacy which, to an extent, would hypothetically legally justify the use of a shutdown. There are recent shutdowns, for example, ordered by the military junta in Myanmar since the coup d'etat in 2021, where issues of the legitimacy of authority become debatable. While the doctrine of rational-legal authority implies that those put in power with actions justified under codified law, there is still the question of proportionality and how a shutdown should be balanced against other forms of censorship, especially within the context of social contract theory, but also other rights, such as the right to access to information.

Shutdowns are one of many methods by which actors (usually governments) exert power and control over data flows within their digital domain. Acknowledging the partially borderless nature of the Internet and that shutdowns are often implemented by state orders to Internet Service Providers (ISPs) located within a nation's physical border, to a large degree, shutdowns are limited at the country level. A single shutdown event affecting more than one country or a country other than the ordering state has not yet been recorded and may have legal issues due to an infringement of another country's sovereignty.

2.2 The Etymology of Internet Shutdown

The term "internet shutdown" consists of "internet" and "shutdown". The word "internet" comes from "inter" (as a prefix, Latin for among/between) and "network"[1] (usually to represent something similar to a net, e.g. see opus reticulatum)[2]. One of its earliest uses of the term "internet" was in 1974 when describing an "Internetwork Transmission Control Program (TCP)". An inter-network is 'between networks', which is why the Internet is often referred to as a network of networks.[3] The term "shutdown" comes from "shut" (skutjan, West Germanic) and "down" (ofdune, Old English). Initially often used in reference to machines in the industrial revolution, the term "shutdown" has since developed and currently can have a wide range of applications, such as a government shutdown, to being shut down in an argument, to a factory shutdown, and more recently, an internet shutdown.

2.3 History of Internet Shutdowns

The use of the term "internet shutdown" is often traced back to the Arab Spring of the early 2010s, when several governments in the Arab world ordered ISPs to disable their services in an attempt to quell protests and other forms of collective action which called for social, economic, and political change. These state-ordered internet shutdowns brought the term "internet shutdown" and the unique method of digital repression to the forefront of global media. However, an important framing is found a few years prior.

Internet censorship pre-dates many of the examples discussed in this paper, for example, the 1996 orders by the Zambian government to remove an online edition of a newspaper due to public security concerns [10]. Legislation related to internet censorship can also be found in the 90s, such as the 1996 Communications Decency Act (CDA) and 1998 Child Online Protection Act (COPA). Within specific jurisdictions,

[1] Network can also be split into "net" and "work".
[2] Can be further split into "net" and "work".
[3] See ARPANET to learn more about the Internet's early history.

such as India, the Telegraph Act of 1885 and Section 144 of the Criminal Procedure Code of 1973 are both often used as justifications for internet shutdowns. While this paper is not focused on the legal means by which shutdowns are justified, it is important to note the rapidly changing nature of the internet against the background of lagging legal frameworks.

This context leads to the common discussion of balancing citizens' rights. For example, in '90s, the European Commission, in light of legislation on "Illegal and harmful content on the internet", had emphasised the same issue which many scholars raise, namely, "the need to strike the right balance between ensuring the free flow of information and guaranteeing protection of the public interest" [18]. With this in mind, when specifically focussing on "internet shutdowns", as we view them, namely to stifle two-way communication, the story begins in the mid-2000s.

With the creation of Facebook in 2004, YouTube in 2005 and Twitter in 2006, the world saw its first recorded "internet shutdown" in February 2007 when protests calling for the resignation of the Guinean president Lasana Conté gained traction. These protests led to orders for the country's ISPs to shut down the Internet [12].[4] A few months later, in September 2007 in Burma (now Myanmar), shutdowns took place during the "Saffron Revolution" [30]. Based on the chronological sequence of events, the rise of internet shutdowns appears to align with the transition from Web 1.0 to Web 2.0. The affordances provided by the newly established ability for two-way communication and its potential impact on collective action [28] and connective action [8] may explain this apparent correlation.

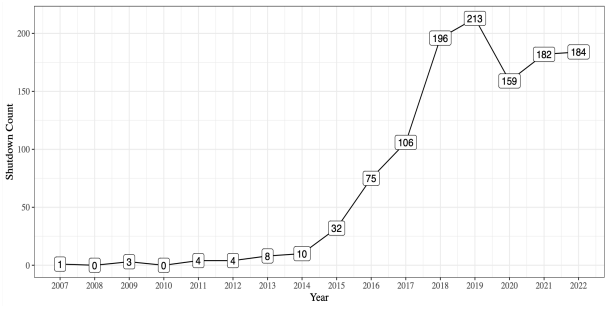

Figure 2: Internet Shutdowns between 2011 and 2022

Since 2007, internet shutdowns began to creep into the digital repression toolbox of countries seeking to control online information, for example, Internet throttling in Iran in 2009 [33], website blocking in Tunisia in 2010 [14] and most notably, the large-scale Internet blackouts in Egypt in 2011.

While some claim Internet kill switches or blackouts were recorded as far back as 2005, we could not find evidence to support these claims. It could be that these journalists were referring to internet filtering. While there was a report on internet filtering in 2005 in Burma (Myanmar), this report does not mention kill switches, blackouts, shutdowns, or any alternative terms to what most currently refer to as internet shutdowns. It is unclear exactly when the term started being used, and as with most terms, is an organic and constantly evolving part of the internet freedom community's diction.

Most references to an "internet shutdown" that pre-date 2007 often discuss it within the context of cyber-attacks, either offensively or defensively. For example, when an "internet shutdown was triggered by an "apparent cyber terror committed by hackers" [7], or to use a shutdown to mitigate the damage and spread of a cyber-attack as proposed by the White House in 2004. With warnings about the increasing risk of a potential "Cyber Pandemic", we may see the cyber security argument increasingly become a justification for implementing an internet shutdown. Another common use of the term "internet shutdown", which pre-dates 2007, refers to unintentional network issues such as top-level domain failures.

When discussing alternatives to "Internet shutdowns", the terminology can be traced back further. Mentions of "Internet blackout" that pre-date 2007 are often within the context of DDoS attacks, e.g., Slammer worm in 2003, or in entertainment, for example, is the 1998 X-Files episode titled "Kill-Switch", written by William Gibson and Tom Maddox. However, in this example, "Kill-Switch" refers to code designed to destroy a malevolent AI. Other mentions within the entertainment sector can be found in the novel "Pirate Cinema" by Cory Doctorow, whereby due to copyright infringements by the antagonist, the authorities "took away my family's Internet and ruined our lives" (p.14). Within a context of collective action, examples of related terms include the 1996 "Turn the Web Black" protests, the 2007-2009 "Shutdown Day" campaign, and the 2012 "Internet Blackout Day". These examples highlight the terminological breadth and that the current use term of the "Internet shutdown" may have been developed from a combination of science fiction, anti-censorship protests, and cyber-security concerns.

Given the relationship between two-way communication and its affordances for collective action, combined with shutdowns, which are commonly used for quelling protests or riots [13], this paper primarily discusses internet shutdowns within the context of information control of online two-way communication.

3 Terminologies

Please view the Appendix for a list of relevant "internet shutdown" definitions and related terms.

3.1 Overview

Access Now has proposed two definitions for an "internet shutdown", one in 2016 and another in 2022. Both are some of the most referenced in academia and media. This, in part,

[4] Lasana Conté also ordered the blocking of print and broadcast media.

is explained by their strong advocacy focus and KeepItOn coalition, which comprises over 300 organisations in 105 countries. Given their global coalition, it is worth breaking down their definition's constituent parts and highlighting how it developed over time. This development may reflect the broader community as both definitions were developed with input from community members.

Access Now's 2016 definition is:

An internet shutdown is an:

1. intentional disruption of Internet or electronic communications,
2. rendering them inaccessible or effectively unusable,
3. for a specific population or within a location,
4. often to exert control over the flow of information.

Access Now's 2022 definition is:

An internet shutdown is an:

1. interference with **electronic systems**
2. primarily used for **person-to-person communications**,
3. intended to render them inaccessible or effectively unusable,
4. to exert control over the flow of information.

Firstly, note the change from "internet or electronic communications" to "electronic systems". Both refer to the electronic nature of the shutdown, and as such, non-electronic censorship acts such as hard copy book banning would not classify as an internet shutdown. Secondly, the addition of "person-to-person communications" implies that blocking one-way websites, such as Wikipedia, would not constitute an internet shutdown. Thirdly, the element that the internet shutdown impact is "inaccessible or effectively unusable" highlights various types of shutdowns, as severe internet throttling will the Internet effectively unusable. Lastly, to "exert control over the flow of information" speaks to the intention of the shutdown, meaning shutdowns for any other purposes besides information control would not qualify under this definition, for example, network maintenance or lack thereof due to negligence.

The 2019 Internet Society definition builds on Access Now's 2016 definition, which they acknowledge in a footnote, and is broadly similar with slight changes, which are highlighted below:

An Internet shutdown is an:

1. intentional disruption of **Internet-based** communications,
2. rendering them inaccessible or effectively **unavailable**,
3. for a specific population, location, **or mode of access**,
4. often to exert control over the flow of information.

Specifically, they change "internet or electronic communications" to "internet-based communication", "unusable" to "unavailable", and include the addition of "mode of access".

The 2016 AfriSIG definition was developed a few months after the 2016 Access Now definition and differentiates itself as it specifies the actors perpetrating the internet shutdown, namely the specification of "state or non-state actors", as highlighted below.

An internet shutdown is an

1. intentional interruption of the Internet by **state or non-state actors**
2. which renders the Internet inaccessible or effectively unusable,
3. for a specific population and
4. for the purposes of exerting control over the free flow of information.

The 2022 UNHCHR definition is as follows:
Internet shutdowns are:

1. measures taken by a government, or on behalf of a government,
2. to intentionally disrupt access to, and the use of, information and communications systems online.
3. They include actions that limit the ability of a large number of people to use online communications tools,
4. either by restricting Internet connectivity at large or by obstructing the accessibility and usability of services
5. that are necessary for interactive communications, such as social media and messaging services.

Here we note the specification of the government's role in enacting the shutdown, either directly or indirectly. Similar to other definitions, they also specify intentionality and online information and communications systems. This definition also specifies scale, namely the "large" scale of the event, and rather than adopting the wording of "two-way" communication, opts for "interactive communications" and specifies "social media and messaging service".

The 2017 AFRINIC proposed definition, which eventually failed to be adopted by the body, was:
An internet shutdown is deemed to have occurred when:

1. it can be proved that there was an attempt, **failed or successful**,
2. to restrict access to the Internet
3. to a segment of the population
4. irrespective of the provider or access medium that they utilise.

Interestingly, this definition includes the phrasing of "an attempt, failed or successful".

The definition provided as part of Olukotun's blog post for DW Akademie is mostly the same as Access Now's 2016 definition, as they were Access Now's Senior Global Advocacy Manager at the time of publication. However, we note that part of the blog post states, "Internet shutdown happens when someone – usually a government – intentionally disrupts the Internet or mobile apps like WhatsApp or Telegram to control what people say online" and "shutdowns are also sometimes called "blackouts" or "kill switches"". This is notable given their previous position within the NGO as they imply blackout and kill-switches are synonymous with internet shutdowns. This same list of terms is reflected in TRT World's article on shutdowns: "Also known as blackouts or kill switches, internet shutdowns are when an entity, like a government or non-state actor, intentionally disrupts access to the Internet or certain apps, in order to control the flow of information in a country or region."

In addition to the above definitions of "internet shutdown", many articles make the specification of a "government-led", "government-imposed", or "government-run" [9] internet shutdown, which implies the existence of a non-government-imposed shutdown. As some definitions specify that a non-state actor can cause a shutdown, there is potential value in further research exploring the extent to which state and non-state actors cause an internet shutdown and the types of non-state actors responsible.

Furthermore, the terms discussed in this paper are often discipline-dependent, and it is unlikely that consensus will be reached across the entire community. It is more likely that several definitions will be used in practice, for example, a technical vs social definition. From ISPs to legal scholars to civil society, a different definition will likely be referenced based on the purpose at hand, should it be for advocacy, legal or other reasons.

Beyond terms laid out in the Appendix, many media articles, when discussing restricted access to the Internet, have referred to alternative phrases, such as "internet cutoff" [32], "web shutdown" [20], or "digital blackout" [44]. From another perspective, in the context of electricity voltage, terms such as a "blackout" usually refer to an unintentional complete outage, or "brownouts" refer to either an intentional or unintentional outage. While there are several terms in the Appendix which should likely be redefined or consolidated, for the sake of brevity, we will discuss two examples below, digital curfew and digital siege.

First, "virtual curfews ... happen when telecommunications infrastructure, including mobile or Internet networks or both, are shut off or disrupted deliberately." [37]. We believe that reframing "virtual curfews" to reflect the colloquial use of the term "curfew" could be helpful. Just a digital curfew refers to a time by electronic appliances are not used, for example, the daily "digital detox" each evening for 1.5 hours in a village in Sangli, Maharashtra, India [40], a virtual curfew implies a consistent time of day whereby the Internet is not used, whether voluntarily or not. However, as with most curfews, the term itself implies that it has been announced beforehand. This is often not the case with internet shutdowns, as many are reactive [36]. When they are preventative, there is often a lack of formal announcement that a shutdown is expected. Lastly, curfews often last longer than a single day, and many shutdowns are relatively short, lasting a day or two. Given the use of the term "curfew" and that shutdowns use does not align with other uses of the term "curfews", this term could be redefined to a specific type of shutdown. For example, a new definition could include some form of its preventative nature, announced ahead of time, and perhaps cyclical.

This idea of cyclical internet shutdown is reminiscent of "rolling blackouts" or "rotating outages". While these terms are mainly caused to balance the supply and demand of electricity, adopting such terminology in the case of internet shutdowns could be reasonable. For example, where an "internet curfew" could refer to a more daily internet shutdown, we could have "rolling internet shutdowns" on a broader time space, e.g. weekly, monthly, or yearly at consistent intervals.

Second, a "digital siege" comes into being when a "blackout is maintained for more than one week" (p. 120) [34]. However, to consolidate the terminology, it may be reasonable to take the idea of a digital siege and apply a consistent phrasing based on the type of shutdown. For example, a "prolonged" or "sustained" internet blackout, network shutdown, platform blockage or internet slowdown.

3.2 The Four Pillars of Internet Shutdowns

The Four Pillars of Internet Shutdowns, visualised in Figure 3, is a four-part framework to understand the primary types of internet shutdowns and how they fit into the broader literature.

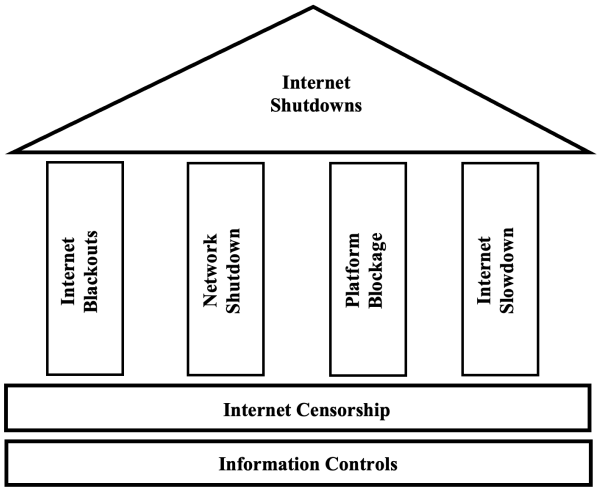

Figure 3: The Four Pillars of Internet Shutdowns

Firstly, the framework's foundation is built on "information controls", which encompasses all types of censorship, both offline and online. Secondly, internet censorship is built on information controls and specifies the medium of censorship. Specifically, internet censorship would not encompass censorship through other digital means, such as telex or radio. Thirdly, there are four pillars (archetypes of shutdowns) that can refer to most types of intentional internet disruptions in one regard or the other. These are (1) internet blackout, (2) network shutdown, (3), platform blockage, and (4) internet slowdown. Lastly, to refer to these four terms more generally, and given its' consistent use with media and the United Nations, there is value in keeping the term "internet shutdown" as an umbrella term and can be used when referring to any or multiple of the four pillars.

The four pillars mainly refer to the following definitions;

1. *Internet Blackout*
   An "internet blackout" is the cessation of all internet services across all networks and platforms. This could be considered an alternative term to "full shutdown".

2. *Network Shutdown*
   A "network shutdown" is the cessation of all internet services on a specific network, such as mobile or fixed-line broadband. This could be considered an alternative term to "partial shutdown".

3. *Platform Blockage*
   A "platform blockage" is blocking a specific platform used for two-way communication, such as a social media app. This could be considered an alternative term to "partial shutdown". Blocking of other websites, non primarily intended for two-way communication, would rather be classified as general filtering.

4. *Internet Slowdown*
   An "internet slowdown" is a type of shutdown if the bandwidth/throughput falls below a specific threshold [5] rendering internet use impractical. This could be considered an alternative term to "internet throttling".

To reiterate, these four pillars are intended for future researchers to be able to consistently differentiate between types of "internet shutdowns" more systematically than is currently available. This will make future data analysis between and within similar types of internet shutdowns easier. Without adopting the Four Pillars, or a similar approach, could result in future researchers continuing to bucket all types of shutdowns in the same category, which is often the case in social science research.

[5] For example, could be a 2G threshold given "governments increasingly resort to throttling bandwidth or limiting mobile service to 2G, which, while nominally maintaining access, renders it extremely difficult to make meaningful use of the Internet" (p.2) [27]

4 Taxonomies

Various taxonomies of shutdowns exist. Some are more technical than others, and each taxonomy provides a unique value add, dependent on the context and purposes for which one is looking to analyse internet shutdowns. Below is a brief overview of several shutdown or outage taxonomies.

Access Now's report "Taxonomy of internet shutdowns: the technologies behind network interference" [3] identifies eight types:

1. Fundamental Infrastructure Shutdown
2. Domain Name System (DNS) Manipulation
3. Throttling
4. Deep Packet Inspection (DPI)
5. Routing
6. Filtering
7. Rogue Infrastructure Attack
8. Denial of Service (DoS) Attack

Feldstein's paper "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?" [19] identifies eight types of network disruptions and Internet blocking techniques:

1. Full or Partial Blackout
2. Domain Name System (DNS) Interference
3. Throttling
4. Deep Packet Inspection (DPI)
5. IP and Protocol-based Blocking
6. URL-Based Blocking
7. Platform-Based Blocking
8. Non-technical Strategies

Thousand Eyes' eBook "The Internet Outage: Survival Guide" [41] discusses ten causes of outages grouped into three categories:

1. Internet Routing Outages
   (a) BGP Route Hijack
   (b) BGP Route Leak
   (c) BGP Route Flap
2. Reachability Outages
   (a) DDoS Attack
   (b) DNS Hijacks Cache Poisoning
3. Internet Cloud Network Outages
   (a) ISP Infrastructure
   (b) Cloud Provider Network
   (c) Natural Disaster
   (d) Operator Error

(e) Internet Sovereignty

The Internet Society's report "Perspectives on Internet Content Blocking" [22] discusses five types of application or content blocking techniques which are listed below.[6]

1. IP and Protocol-Based Blocking
2. Deep Packet Inspection-Based Blocking
3. URL-Based Blocking
4. Platform-Based blocking (Especially Search Engines)
5. DNS-Based Blocking

The Internet Society specifies that "Internet shutdowns are different than application-level or content censorship/blocking, where Internet connectivity is available, but access to selected websites or applications is limited." Moreover, in their policy brief on internet shutdowns, they state, "for the purposes of this briefing document, application/content blocking should be considered separate and distinct." Notably, the Internet Society's taxonomy on application or content-blocking techniques is very similar to many of the other taxonomies and emphasises that shutdowns and application or content-blocking techniques are uniquely distinct.

Surfshark highlights four blocking techniques in their website's "Blocking FAQ" [38]

1. IP Blocking
2. DNS Blocking
3. Deep Packet Inspection (DPI)
4. HTTP-Based Blocking

As part of their dashboard, they have an "Internet Shutdown Tracker" with a description of "Undemocratic governments around the world are increasingly turning to internet blackouts and social media censorship to maintain their rule. They use it to prevent the dissemination of information and to impede organizational efforts." Additionally, an "Internet Censorship" page with a description of "when it comes to online censorship, restricting individual platforms isn't that effective because people can always find alternatives. That's why some countries use the nuclear option of disrupting the Internet altogether. This page is meant for tracking such cases specifically." Their internet censorship page's data is the same as their shutdown page when selecting "disrupted internet connection in the past." [7]

Google Jigsaw's (2023) "The Current" lists six primary methods of shutdowns:

1. Throttling
2. IP Blocking
3. Mobile Data Shutoffs
4. DNS Interference
5. Server Name Identification Blocking
6. Deep Packet Inspection (DPI)

Top10VPN includes three types of disruptions in their annual "Cost of Internet Shutdowns" report:

1. Internet Blackouts
2. Internet Throttling
3. Social Media Blocks

The types of shutdowns used by Top10VPN are similar to the aforementioned "Four Pillars of Internet Shutdowns". However, we believe the addition of "Network Shutdown" and rewording the other types are worthwhile changes.

West's (2016) article "Internet shutdowns cost countries 2.4 billion USD last year" identifies six types of shutdowns:

1. National Internet
2. Subnational Mobile
3. National Apps/Services
4. Subnational Internet
5. National Mobile
6. Subnational Apps/Services[8]

West's six categories of shutdowns focus on two aspects, geographic scope (national vs subnational) and the affected network (e.g. mobile vs landline). This taxonomy is notably different from the other taxonomies, and we believe there is value in further classifying different types of shutdowns in this fashion, as discussed in more detail below.

Before delving into the taxonomy, we turn to the paper "Spectrum of Shutdowns: Reframing Internet Shutdowns From Africa" by [25], which calls for a reframing of internet shutdowns to account for the grey areas surrounding shutdowns. They identify four variables to understand shutdowns:

1. Frequency and Duration,
2. Depth,
3. Breadth, and,
4. Speed.

[6] See Internet Society's "Perspectives on Content Blocking: An Overview for additional information on such actions."

[7] Their options for past disruptions on internet service past restriction on social media and voice communication, and current restriction social media and voice communication all show different data.

[8] From 1 to 6, the number of occurrences were 36, 22, 14, 7, 1, 1

These variables are respectively concerned with; "how often and for how long the Internet is shut off in a particular place; the type of content that is targeted; how many people are affected or how geographically dispersed a shutdown is; and techniques available to implement shutdowns". While this increased granularity is a step in the right direction, there are areas to improve or develop these variables. Firstly, "Frequency and Duration" should be split as they refer to fundamentally different elements of shutdowns. Recall the differences between a virtual curfew and digital siege, focusing on frequency and duration elements, respectively. Secondly, rewording of what constitutes each of these variables. For example, the term "Speed", to refer to techniques available to implement shutdowns, should be rephrased to a description to refer to bandwidth and throughput level relative to a certain threshold determined by, for instance, a regional or national average. Which, if it falls below a certain level, may indicate throttling. The authors mainly discuss a few variables of which we can discuss shutdowns, not types of shutdowns. However, their framing of a spectrum is helpful in understanding that shutdowns have varying degrees. For example, "Depth" can vary from mild throttling to complete blackout. With these degrees in mind, many other variables can be seen on a spectrum, for example, the geographical scope or number of people affected. Was it short (e.g. less than three days) or long (e.g. longer than two weeks)? Figure 4 shows a few variables we can use to analyse a shutdown as a spectrum rather than dichotomously.

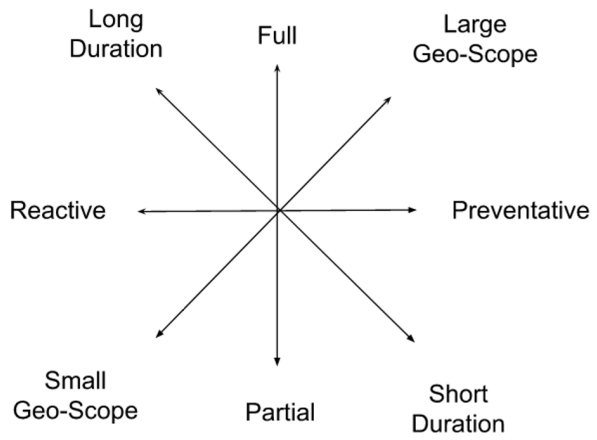

Figure 4: Different Spectrum Variables to Analyse Shutdowns

Figure 4 goes beyond to common dichotomous approach to shutdowns in the social science literature, namely, between a "Full" or "Partial" shutdown. Whereas a partial shutdown can be used to describe the ban of specific social media platforms, for example, the ban of WhatsApp and Twitter in Chad between 2018-2019 [4]. A full shutdown refers to a more indiscriminate form, for example, in 2021, when a large degree of Kazakhstan became disconnected as a result of protests [35]. Building on the notion of placing shutdowns on a one-dimensional space (a line or spectrum), there is potential to reframe shutdowns in a two-dimensional or even a three-dimensional space, which will conceptually create 4 or 8 quadrants, respectively. Based on the variables chosen to create these quadrants, most shutdowns, to an extent, should be able to be classified. For example, to classify a large geographic scope, long duration and full depth shutdown is Type 1A, or a small geographic scope, short duration and partial shutdown is Type 2D. See Table 1 for more examples.

4.1 A Taxonomy of Shutdowns for Social Data Scientists

There are a few variables which are more feasible to determine than others. For example, the affected geographic scope or the shutdown duration. Other variables, such as reactive or preventative (intent to an extent), are substantially more difficult to determine given the opacity of the shutdown decision-making process.

	Geo-Scope	**Duration**	**Depth**
Type 1A	Large	Long	Full
Type 1B	Large	Long	Partial
Type 1C	Large	Short	Full
Type 1D	Large	Short	Partial
Type 2A	Small	Long	Full
Type 2B	Small	Long	Partial
Type 2C	Small	Short	Full
Type 2D	Small	Short	Partial

Table 1: Types of Shutdowns, Three Variables, Two Buckets

We acknowledge that the above approach would only allow up to 8 types with three dichotomous variables. However, if more granularity is needed, bucketing variables into small, medium, and large geographic scope could be a path forward.

	Geo-Scope	**Duration**
Type 1A	Large	Long
Type 1B	Large	Medium
Type 1C	Large	Short
Type 2A	Medium	Long
Type 2B	Medium	Medium
Type 2C	Medium	Short
Type 3A	Small	Long
Type 3B	Small	Medium
Type 3C	Small	Short

Table 2: Types of Shutdowns, Two Variables, Three Buckets

When combined with the concept of the four pillars, the granularity of the classification would increase accordingly.

For example, a large geographic scope and long duration of severe internet throttling would be a Type 1A Internet Slowdown, or a small geographic scope and short duration blocking of a social media platform would be a Type 3C Platform Blockage. While there will always be edge cases, the main advantage of the classification methods proposed in this paper is that it goes beyond what is currently used within the literature and, if adopted, should improve the methodological consistency across the community.

5 Discussion and Limitations

Firstly, it is essential to note the dynamic nature of internet shutdowns. A shutdown can often present an "adaptive" challenge to a network [11]. For example, a shutdown which starts as an internet slowdown might evolve into a network shutdown and then an internet blackout. As such, there are limitations to classifying shutdowns using this approach, given that the real-world implementation of a shutdown is often reactive to the development of external forces, such as a protest deteriorating into a riot.

Second, as the four pillars simplify the real world, it will be difficult to decide where a shutdown event belongs in many cases. To account for all unique cases would be impractical and limit our frameworks' applicability. Furthermore, determining the exact nature of a shutdown is difficult and is often done after the fact. As such, this approach is limited given its rigidity, and it may only be suitable in historical cases where enough data is available to determine shutdown type, scope and impact area. However, it presents a reasonable starting point for researchers looking to adopt a more consistent methodological approach to studying internet shutdowns.

Thirdly, determining the cut-off point for what constitutes a large-medium-small geographic scope or short-medium-long duration is subjective. However, it is possible to adopt cut-off points already determined by others. For example, Access Now's STOP data distinguishes between three types of geographic scope. A shutdown that 1) only affected one city, county, or village, 2) affected more than one city in the same state, province, or region, and 3) affected locations in more than one state, province, or region. Equally, given the vast differences in population density and internet penetration, one might aim to determine the scope based on the number of affected users. Regarding duration, one could use data analysis to determine cut-offs. For example, in a previous paper we determined that most shutdowns in India (the leading country in terms of recorded shutdowns) are no longer than three days [13], making a sub-3-day shutdown "short". Or to use existing literature, such as Rydzak's digital siege, which uses a 2-week length for a prolonged shutdown, which could determine what a "long" shutdown.

Lastly, given the rapidly evolving field of internet freedom research, partly due to the technological development of communication, censorship, and circumvention methods, we acknowledge there are shifting objectives or priorities for various stakeholders, from NGOs to government, to ISPs. As a result, the approaches described above will likely need to be revisited and built upon as the landscape of information controls changes.

6 Conclusion

This paper explored the terminologies and taxonomies of internet shutdowns and provided a brief historical context and review of existing approaches, proposing two novel non-technical frameworks. The first was the "Four Pillars of Internet Shutdown", which described four archetypes of shutdowns that all fall under the umbrella term of "internet shutdowns", namely 1) internet blackout, 2) network shutdown, 3) platform blockage, and 4) internet slowdown. The second described a systematic way to group shutdowns, for example, based on geographic scope, duration, or depth. These approaches would enable, for example, computational social scientists to analyse between and within similar shutdowns in a methodologically principled manner. This paper provided a novel addition to the literature because it explored the grey areas between shutdown definitions and synonyms, and provided two potential ways forward for researchers and policymakers to better understand the wide range of internet shutdowns that exist.

References

[1] ACCESS NOW. Rightscon 2016 outcomes report, 2016.

[2] ACCESS NOW. Glossary: Definition of internet shutdowns, 2022.

[3] ACCESS NOW. A taxonomy of internet shutdowns: The technologies behind network interference, 2022.

[4] ADEBAYO, B. After a 16-month blackout, chad is back on facebook, twitter and other social platforms. *CNN* (2019).

[5] AFRICAN SCHOOL ON INTERNET GOVERNANCE. Statement on intentional internet shutdowns, 2016.

[6] AFRINIC. Anti-shutdown-01.

[7] BBC. Virus-like attack hits web traffic. *BBC* (January 2003).

[8] BENNETT, W. L., AND SEGERBERG, A. *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*. Cambridge University Press, 2012.

[9] BERGIN, J., AND LIM, L. Flicking the kill switch: governments embrace internet shutdowns as a form of control. *The Guardian* (Aug 2022).

[10] BURNHEIM, S. The right to communicate: The internet in africa, censorship and control: Obstacles to growth. *South African Journal of Information and Communication 7*, 1 (2006), 10.

[11] CETINKAYA, E., AND STERBENZ, J. A taxonomy of network challenges.pdf.

[12] CIPESA. Despots and disruptions: Five dimensions of internet shutdowns in africa.

[13] COLLYER, M., AND WRIGHT, J. A bayesian analysis of collective action and internet shutdowns in india.

[14] COMMITTEE TO PROTECT JOURNALISTS. Tunisia must end censorship on coverage of unrest.

[15] COMPUTER LANGUAGE. Internet blackout—clc definition, 2023.

[16] DENARDIS, L. *The Global War for Internet Governance*. 2014.

[17] DUSZA, K. Max weber's conception of the state. *International Journal of Politics, Culture and Society 3*, 1 (1989), 71–105.

[18] EUROPEAN COMMISSION. Illegal and harmful content on the internet, 1996.

[19] FELDSTEIN, S. Government internet shutdowns are changing. how should citizens and democracies respond?, 2022.

[20] FIERCE WIRELESS. Web shutdown cost egypt €81.

[21] INTERNET FREEDOM FOUNDATION. Faq on internet shutdowns.

[22] INTERNET SOCIETY. *Internet Society Perspectives on Internet Content Blocking: An Overview*. 2017.

[23] INTERNET SOCIETY. *Internet Shutdowns: An Internet Society Public Policy Briefing*. 2019.

[24] KAYE, D. Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. *A/HRC/35/22* (2017).

[25] MARCHANT, E., AND STREMLAU, N. A spectrum of shutdowns: Reframing internet shutdowns from africa. *16* (2020).

[26] NOW, A. *Internet Shutdowns and Elections Handbook*. Access Now, 2021.

[27] OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. Internet shutdowns: Trends, causes, legal implications and impacts on a range of human rights. *Report of the Office of the United Nations High Commissioner for Human Rights* (2022).

[28] OLSON, M. The logic of collective action.

[29] OLUKOTUN, D. B. Internet shutdowns – an explainer. *DW.COM* (2016).

[30] OPEN NET INITIATIVE. Pulling the plug: A technical review of the internet shutdown in burma.

[31] OPEN OBSERVATORY OF NETWORK INTERFERENCE. Ooni glossary.

[32] REED, J. Syrian internet cutoff may be precursor to assad offensive. *Foreign Policy* (2012).

[33] RHOADS, C., FOWLER, G. A., AND CUMMINS, C. Iran cracks down on internet use, foreign media. *WSJ* (2009).

[34] RYDZAK, J. A. A total eclipse of the net: The dynamics of network shutdowns and collective action responses.

[35] SKOK, A., KRAPIV, N., AND ZHYRMON, A. Kazakhstan internet shutdowns and protests: Timeline. *Access Now* (January 2022).

[36] SOFTWARE FREEDOM LAW CENTRE. Internet shutdowns. https://internetshutdowns.in/.

[37] SRIVASTAVA, R. Anatomy of virtual curfews: Human rights vs. national security.

[38] SURFSHARK. Internet Censorship Around the World: Statistics and Research. https://surfshark.com/research/internet-censorship.

[39] SUTTERLIN, E. Flipping the kill-switch: Why governments shut down the internet.

[40] THE ECONOMIC TIMES. Digital detox: A maharashtra village holds a lesson for all of us. *The Economic Times* (September 2022).

[41] THOUSAND EYES. The internet outage survival guide: Unpacking common outages types and how they impact your business.

[42] TRT WORLD. Explained: How do internet shutdowns work? *Explained: How Do Internet Shutdowns Work?* (2021).

[43] WEST, D. M. Internet shutdowns cost countries 2.4*billionlastyear.*

[44] WRIGHT, C. Turn on, turn off: Understanding iran's digital blackout. *WIRED Middle East* (October 2022).

7 Non-Exhaustive List of Terms

Term	Definition
Internet Shutdown	"An internet shutdown is 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" [2]
Internet Shutdown	"An internet shutdown is an interference with electronic systems primarily used for person-to-person communications, intended to render them inaccessible or effectively unusable, to exert control over the flow of information." [1]
Internet Shutdown	"An Internet shutdown is an intentional disruption of Internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information." [23]
Internet Shutdown	"An internet shutdown is an intentional interruption of the Internet by state or non-state actors which renders the Internet inaccessible or effectively unusable, for a specific population and for the purposes of exerting control over the free flow of information" [5]
Internet Shutdown	"Internet shutdowns are measures taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online. They include actions that limit the ability of a large number of people to use online communications tools, either by restricting Internet connectivity at large or by obstructing the accessibility and usability of services that are necessary for interactive communications, such as social media and messaging services." [27]
Internet Shutdown	"Internet shutdowns are an absolute restriction placed on the use of internet services due to an order issued by a government body. It may be limited to a specific place and to specific period, time or number of days. Sometimes it can even extend indefinitely. An internet shutdown may be limited to mobile Internet that you use on smartphones, or the wired broadband that usually connects a desktop - or both at the same time." [21] OR "Internet shutdowns are extraordinary measures which are used by repressive, authoritarian regimes to limit flows of information." [21]
Internet Shutdown	"An internet shutdown is deemed to have occurred when it can be proved that there was an attempt, failed or successful, to restrict access to the internet to a segment of the population irrespective of the provider or access medium that they utilise." [6]
Internet Shutdown	"An Internet shutdown happens when someone – usually a government – intentionally disrupts the Internet or mobile apps like WhatsApp or Telegram to control what people say online. . . .Shutdowns are also sometimes called "blackouts" or "Kill switches"" [29]
Internet Shutdown	"Also known as blackouts or kill switches, internet shutdowns are when an entity, like a government or non-state actor, intentionally disrupts access to the Internet or certain apps, in order to control the flow of information in a country or region." [42]
Internet and Telecommunications Shutdowns	"Internet and telecommunications shutdowns involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law (see A/HRC/32/13, para. 10)." [24]
Blanket Shutdown	"A blanket shutdown or a total blackout is a disruption where internet access is cut entirely." [26]
Total Blackouts	"A blanket shutdown or a total blackout is a disruption where internet access is cut entirely." [26]
Internet Blackout	"An internet shutdown or an internet blackout is 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." [26]
Internet Outage	"An outage on the Internet caused by an attack on a website, ISP or the Internet's domain naming system (DNS)." [15] or "An outage on the Internet due to an improper configuration of the Web server infrastructure." [15] or "An organised outage on the Internet to make a protest." [15]
Internet Blackout	"An internet blackout (also referred to as "internet outage" or "internet shutdown") occurs when the internet is completely turned-off in a country or region. The area or network affected by the internet blackout has no internet access at all. An internet blackout may be intentional (ordered by a government) – in which case, it constitutes a form of internet censorship – or it may have been caused unintentionally (for example, due to disruption of cables)." [31] An internet blackout may be intentional (ordered by a government) – in which case, it constitutes a form of internet censorship – or it may have been caused unintentionally (for example, due to disruption of cables)." [31]
Partial Shutdown	"Partial shutdowns are disruptions that target specific services such as social media platforms and messaging apps or networks such as mobile networks."accessnow2021handbook
Digital Siege	"A blackout is maintained for more than one week, thus becoming a digital siege" (p. 120) [34]
Virtual Curfew	"Virtual curfews or network disconnections/Internet shutdowns happen when telecommunications infrastructure, including mobile or Internet networks or both, are shut off or disrupted deliberately" (p. 10) [37]
Network Disruption	"Network disruptions target specific or all telecommunication networks as opposed to particular services. For example, they can affect 3G or 4G mobile networks." [26]
Network Interference	"Network interference is an umbrella term used to describe various forms of interference that occur on networks on the internet. Within the OONI context, the term network interference is primarily used to refer to cases of internet censorship and traffic manipulation." [31]
Internet Throttling	"Internet throttling is the practice of intentionally slowing down internet speeds, making it difficult or impossible for users to upload or download information. Throttling can also target specific services, applications, and platforms, rendering them unusable." [26]
Communication Blackouts	"In Chapter 3, I argued that communication blackouts escalate collective action in the short run, but undermine it when they are maintained as a digital siege." (p. 124) [34]
Internet Disruption	"An Internet disruption, often referred to as an internet shutdown, is the intentional blockage of access to the Internet or sections of the Internet such as social media platforms. Internet disruptions are mostly ordered by governments eager to disrupt communications and curtail citizens' access to information in order to limit what the citizens can see, do, or communicate" (p. 2) [12]
Kill-Switch Shutdowns	"kill-switch shutdowns" in which the government turns off the entire internet—that is, blocks all access to fixed-line or mobile internet services, rather than blocking certain websites or applications or merely slowing down internet speeds." (p.10) [39] however, "the monolithic term "kill-switch" is a misnomer, there are numerous points of concentration where outages and disruptions can occur." [16]
Network Interference	"Network interference is an umbrella term used to describe various forms of interference that occur on networks on the internet. Within the OONI context, the term network interference is primarily used to refer to cases of internet censorship and traffic manipulation." [31]
Internet Censorship	"Internet censorship is the intentional control or suppression of what can be accessed, published, or viewed on the internet. Internet Service Providers (ISPs) usually implement internet censorship based on government orders and/or in compliance with national legislation. This involves blocking access to specific websites and/or applications, preventing users of that specific network from accessing specific internet services. As internet censorship is implemented on the network level, it may differ from network to network, and from country to country." [31]