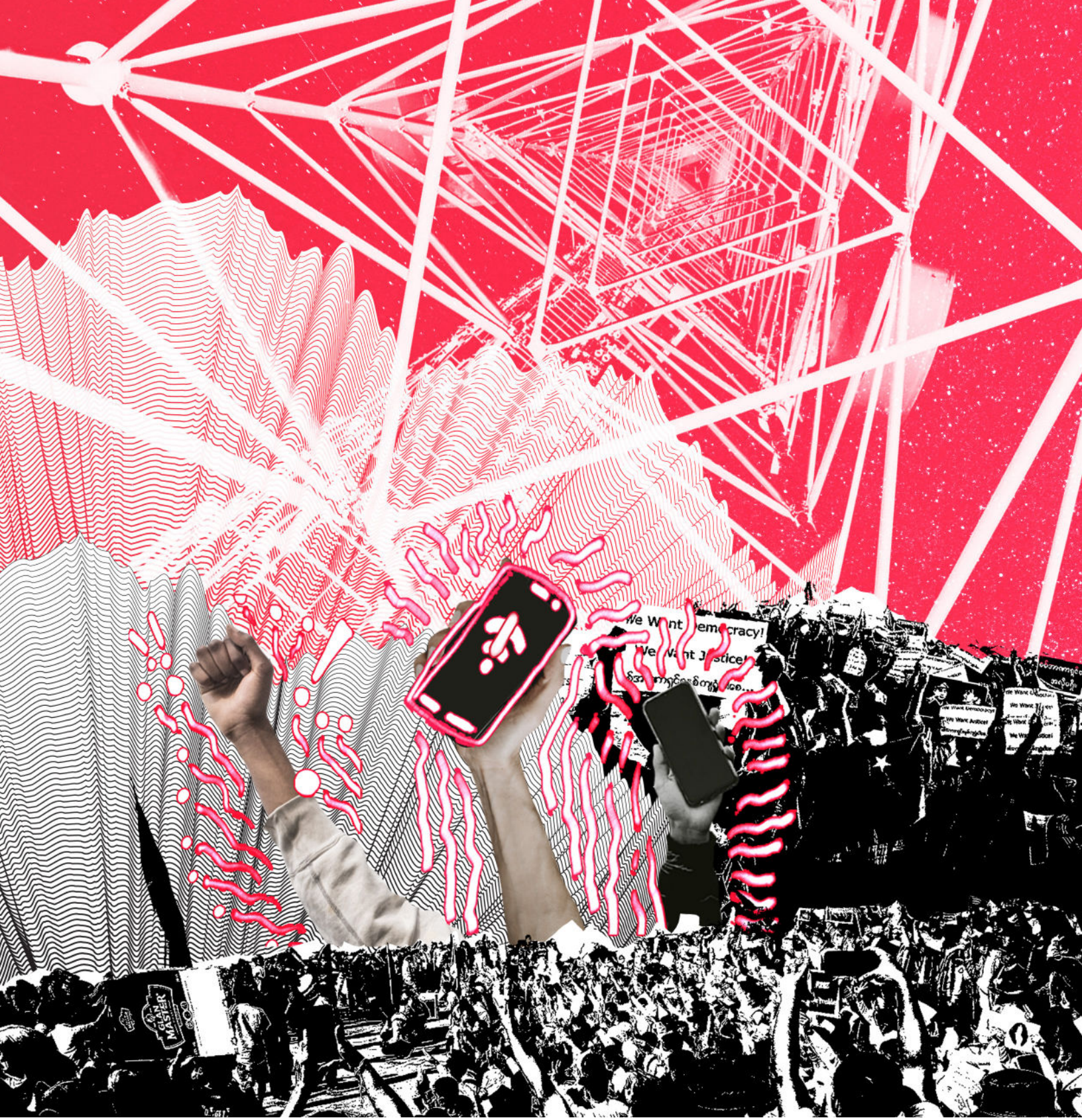


A TAXONOMY OF INTERNET SHUTDOWNS: THE TECHNOLOGIES BEHIND NETWORK INTERFERENCE

#KeepItOn

A taxonomy of internet shutdowns: the technologies behind network interference

This paper is an Access Now publication. It was written by Gustaf Björksten. We would like to thank the Access Now team members who provided support, including Felicia Anthonio, Daniel Bedoya Arroyo, Marianne Díaz Hernández, Zach Rosson, Hassen Selmi, Sage Cheng, Carolyn Tackett, and Donna Wentworth. We would also like to thank our #KeepItOn coalition partners who provided valuable feedback and insight, including Melody Patry, Berhan Taye, Arturo Filastò, and Maria Xynou.

The #KeepItOn coalition represents 280+ organizations from 105 countries, fighting internet shutdowns through grassroots advocacy, direct policy-maker engagement, technical support, and legal interventions.

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

June 1 2022

Table of contents

I. Introduction: the purpose and audience for this guide

Internet shutdowns[1] are impacting the lives of billions of people around the world.[2] They can last for minutes or years, target one specific platform or black out entire networks. No matter what form they take, the central fact remains: they violate human rights[3] and put people at risk.

The harms of internet shutdowns are well documented. They range from blocking the free press and access to life-saving information, to interfering with democratic elections and facilitating coups, to hiding alleged war crimes and genocide.[4] What is not as widely understood is how perpetrators, typically governments, implement shutdowns technically.

This lack of technical understanding impacts our capacity to fight back. When it is not clear what is happening or who is responsible, it is difficult to attribute, anticipate, or circumvent a shutdown. It also makes accountability after the fact that much more difficult.

Internet shutdowns can take many forms, depending on the technology a government or other actor has at its disposal, and what the perpetrator aims to achieve.

In this paper, **we outline each of the various technical mechanisms for implementing a shutdown, and the options for mitigating each type.** Our hope is that **technologists** and **civil society groups** working to end shutdowns will find this a useful technical resource to **understand**, **prepare for, circumvent, and help document deliberate network disruptions.**

[1] An internet shutdown has been defined 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." An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. See Access Now (2020). *No more internet shutdowns! let's #KeepItOn.* Access Now. Retrieved May 11, 2022, from https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/.

[2] Access Now (2022). *Internet shutdowns in 2021: the return of digital authoritarianism*. Retrieved May 16, 2022, from https://www.accessnow.org/internet-shutdowns-2021/.

[3] See Access Now (2022). *#KeepItOn FAQ, Key stakeholder groups, '20. What have international organizations said about internet shutdowns?'* Retrieved May 10, 2022, from https://www.accessnow.org/keepiton-faq/#Key-stakeholder-groups/.

[4] Jigsaw (2021). *The Current: The Internet Shutdowns Issue*. Retrieved May 10, 2022, from https://www.jigsaw.google.com/the-current/shutdown/.

Note that this report **assumes a high level of technological expertise**. It is intended to deepen the knowledge of **technologists** and **digital helpdesk practitioners** seeking to understand how shutdowns work and mitigate their impact. A glossary is available at the end of the document for a brief explanation of acronyms and technical terms used throughout.

Why technical implementation matters ///

Looking at the technical "taxonomy" of internet shutdowns is essential for:

- ➔ Detecting shutdowns when they happen;
- ➔ Identifying where shutdowns are likely to occur; and
- ➔ Developing and deploying effective circumvention tools.

In evaluating how a particular shutdown has been implemented, or whether and how a government or service provider might implement one in the future, we consider four key factors:

1. The technical mechanism used;
2. Where in the network that technical mechanism is implemented;
3. The intended scope of the shutdown — that is, the type of traffic or platform the shutdown is intended to disrupt; and
4. The intended scale (size) of the shutdown — that is, what population is targeted, how much of that population is affected, and where that population is located.

Determining how a shutdown has been carried out can reveal a lot. Not only can it help us determine who is behind the shutdown, it can reveal potential motivations and intent, as well as how likely it is that a perpetrator will continue to hit the kill switch.

The technical mechanisms a government or other actor chooses in a particular context will depend on factors such as how the state's communications infrastructure is organized, the scale of the geographic area the perpetrator is targeting, and the services the state wishes to interrupt. Similarly, where in the network a government implements a shutdown will depend on variables such as its ability to legally compel a communications provider to carry

out a shutdown, the design of the national infrastructure, and the scale of the area and the services it is targeting.

A shutdown implemented by a rogue or malicious actor, meanwhile, will differ in technical implementation from those carried out by nation states, as the perpetrator is less likely to have access or control over the telecommunications infrastructure.

How shutdowns are changing ///

The damage that shutdowns cause may be changing the tactics perpetrators use. Regardless of the official rationale for shutdowns, they cause enormous harm and collateral damage.[5] For example, while a government may proclaim that a shutdown is intended to prevent violence or civil unrest, it may not only fail to meet the stated objective,[6] but also block a population's ability to contact and receive emergency services (physical harm), conduct business (economic harm), and locate missing family members (emotional and psychological harm). In the most egregious cases, internet shutdowns interfere with the right to life.[7] Often, analysis of the circumstances under which a shutdown is ordered suggests the harm and collateral damage is intentional.[8]

As international pressure mounts against this form of "collective punishment,"[9] governments that want to manipulate the flow of information online to censor people or hide their own misdeeds may use targeted shutdowns, throttling, app blocking, or other less obvious forms of disruption, to escape accountability.

For instance, if a government's intention is to prevent a population from sharing images showing civil unrest or state-perpetrated human rights abuses on social media platforms, and the majority of the population connects to these platforms via mobile phones, authorities may shut down mobile data traffic, but leave voice, broadband, and the PSTN (Public Switched Telephone Network) operating.

---

[5] Global Network Initiative (2018). *Weighing The Impact Of Network Shutdowns And Service Restrictions*. Retrieved May 10, 2022, from https://globalnetworkinitiative.org/wp-content/uploads/2018/04/Impacts-Disruptions-EN.pdf/.
[6] Jan Rydzak (2019). *Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India*. Retrieved May 10, 2022, from https://ssrn.com/abstract=3330413/.
[7] Access Now (2020). *#KeepItOn: Internet shutdowns put lives at risk during COVID-19*. Retrieved May 10, 2022, from https://www.accessnow.org/keepiton-internet-shutdowns-put-lives-at-risk-during-covid-19/.
[8] See Access Now (2021). *Internet shutdowns report: Shattered dreams and lost opportunities - a year in the fight to #KeepItOn, Government excuses*. Retrieved May 10, 2022, from https://www.accessnow.org/keepiton-report-a-year-in-the-fight/#tab-3/.
[9] United Nations Human Rights Council (2021). *Ending Internet shutdowns: a path forward*. Retrieved May 10, 2022, from https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_47_24_Add.2_E.pdf/.

How to mitigate shutdowns

The method for mitigating an internet shutdown will depend on the type of shutdown and the particular circumstances. In this paper, we make general suggestions for each type of shutdown we classify. If you are already experiencing or anticipate an internet shutdown in the near future and need emergency technical assistance, we encourage you to contact a CiviCERT helpdesk[10] or Access Now's own Digital Security Helpline ("the Helpline"),[11] a 24/7 resource for civil society across the globe.

II. What is an internet shutdown?

Before we dive into a technical explanation of how internet shutdowns are carried out, it is essential to define what we mean by the term "internet shutdown." The #KeepItOn coalition has historically defined an internet shutdown 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."[12] However, this is not a detailed or technical definition.

This report covers more than what many might consider an "internet shutdown," to address, for example, a deliberate shutdown of a POTS (Plain Old Telephone Service) network or PSTN (Public Switched Telephone Network), or blocking of SMS (Short Message Service) services, neither of which technically involve the internet. Let's unpack our definition of a shutdown to enable a full understanding of the scope of the issue we are examining.

For our purposes in this paper, we consider an internet shutdown to be 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.[13] That means the term would cover actions such as deliberate throttling or

[10] See https://www.digitalfirstaid.org/ for more information.
[11] See https://www.accessnow.org/help/ for more information.
[12] Access Now (2016). *No more internet shutdowns! Let's #KeepItOn*. Retrieved May 10, 2022, from https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/.
[13] This definition came from the 2022 redefinition workshop series conducted by the #KeepItOn coalition, with the aim of capturing the evolving techniques used to implement internet shutdowns,

shutting down of internet access, as well as the blocking of social media or instant messaging platforms. If an act of interference does not fit this definition, we classify it as an act of censorship rather than an internet shutdown.

While shutdowns can be acts of censorship, not all acts of censorship are shutdowns. For instance, we classify the blocking of platforms such as WhatsApp, Facebook, Twitter, and Reddit as internet shutdowns, as each of these platforms are primarily designed for two-way, or multi-way, user-to-user communications. However, we would classify the blocking of platforms such as Wikipedia, Wordpress, or news websites like *The New York Times* as censorship, as we view the primary purpose of these platforms to be for publishing content instead of enabling user-to-user communications.

III. How internet shutdowns are implemented

When a government or rogue actor implements a shutdown, civil society works together to figure out what is happening and help those impacted get connected, document the shutdown, and push those responsible to restore access to the network, apps, or services. Civil society actors include companies and nonprofit groups that detect shutdowns,[14] technologists that work to attribute the shutdowns[15] and assist in circumvention,[16] and rights groups that document and advocate against shutdowns,[17] among others.

When these actors have an understanding of the possible technical implementations for a shutdown, and the reasons an actor may carry out a particular type, they are better equipped to anticipate and help mitigate a disruption. They are also better able to attribute

providing legal clarity, and better navigating the policy advocacy through the complex context across regions, cultures, and regimes. The coalition plans to launch the complete new definition, along with a memorandum and a glossary, as a guiding resource for coalition members, the measurement community, researchers, and investigators, as well as the global movement to end internet shutdowns.

[14] IODA (2021). *Internet Outage Detection and Analysis*. Retrieved May 10, 2022, from https://ioda.caida.org/.

[15] OONI (2022). *Research reports*. Retrieved May 10, 2022 from https://ooni.org/reports/

[16] Access Now Digital Security Helpline (2022). *Digital Security Helpline Services*. Retrieved May 10, 2022, from https://www.accessnow.org/helpline-services/.

[17] See Access Now (2022) *#KeepItOn coalition list*. Retrieved May 10, 2022, from https://www.accessnow.org/keepiton/#coalition/.

a shutdown and gather evidence for holding perpetrators accountable for their actions, including in courts of law[18] or international fora like the United Nations.[19]

To facilitate such understanding, Access Now has created a taxonomy of internet shutdowns for technologists. We identify eight different types of shutdown, based on the method of implementation.[20] For each of the eight types, we provide key information to help technologists prepare for or respond to a shutdown, including information that may be useful for predicting a shutdown in a specific country or region, or attributing the disruption to a particular actor. We also indicate whether the Helpline can be a resource for assistance and mitigation.

The eight types of shutdowns, classified by the technical means, or mechanisms, that authorities use to implement them, are:

1. **Fundamental infrastructure shutdown**
2. **Routing**
3. **Domain Name System (DNS) manipulation**
4. **Filtering**
5. **Deep Packet Inspection (DPI)**
6. **Rogue infrastructure attack**
7. **Denial of Service (DoS) attack**
8. **Throttling**

1. Fundamental infrastructure shutdown ///

We classify any shutdown implemented using a mechanism that is outside the communications system itself, or that is caused by physical damage to the communications infrastructure, as a **fundamental** infrastructure shutdown.

[18] Access Now (2019). *Judges raise the gavel to #KeepItOn around the world*. Retrieved May 10, 2022, from https://www.accessnow.org/judges-raise-the-gavel-to-keepiton-around-the-world/.
[19] See YouTube video (2021). *Statement on the implications of the ongoing situation in the Sudan*. Retrieved May 10, 2022, from https://www.youtube.com/watch?v=3ToedMc1qNA/.
[20] See https://www.ietf.org/archive/id/draft-hall-censorship-tech-07.txt/ for help understanding the different technical mechanisms used to block or impair internet traffic.

How to detect	We can detect fundamental shutdowns on a network, but it can be more difficult to determine the nature of the issue — that is, whether the shutdown is accidental, due to a maintenance failure, or deliberate.
Who can detect them	Companies that track internet traffic flows.[21] The telco that is responsible for the affected communications infrastructure. Individuals, both within the affected population, and external to the affected population, that run network tests.[22]
Detection difficulty	**Hard.** This technique is hard to detect or characterize.
Possible mitigation	In some circumstances, those affected can circumvent a fundamental shutdown using satellite uplinks, packet and digital radio, alternate telecommunications infrastructure, and (in the case of power outage) battery-powered equipment.
Cost of mitigation	**High.** This usually requires significant planning and investment of resources prior to the shutdown.
How the Helpline can assist	The Helpline cannot effectively assist in these circumstances.

Examples of fundamental shutdowns //

→ Turning off the power grid

Example: In the early months of the Arab Spring in Syria, in a context of repression and censorship, the Helpline observed that when there was a street protest, the authorities would often shut down the power grid in the area the protests were to be held.

Example: During elections in May 2013 in Borneo, Malaysia, clients of the Helpline reported that authorities powered off the cell towers providing cellular coverage of key polling stations, in what appears to have been an attempt to stop election monitors from reporting instances of electoral fraud.

[21] Censored Planet (2022). *An Internet-wide, Longitudinal Censorship Observatory*. Retrieved May 11, 2022, from https://censoredplanet.org/.
[22] OONI Probe (2022). *Install OONI Probe*. Retrieved May 11, 2022, from https://ooni.org/install/. https://ooni.org/install/.

Example: In the winters of 2015 and 2016, the Russia-linked hacker group Sandworm caused power outages in Ukraine, which consequently caused shutdowns in communications networks as well.[23]

→ **Destruction of communications infrastructure**

Example: In May 2019, Malawi conducted local and national elections. During the highly contested election, when election results were being transmitted to the electoral commission, numerous internet service providers lost internet connections. According to news reports, perpetrators of the shutdown cut into fiber optics using an axe. The manner in which the cables were cut, the time of the incident, and the specificity of the locations indicate this was not a mere maintenance or accident. These were deliberate actions to disrupt internet connection across the country.[24]

Example: In 2018, a fire that broke out in Orange's technical center in Abidjan, Côte D'Ivoire, destroyed submarine network cables and rendered service inaccessible for weeks. Some media reports said that police found ladders and keys at the site, suggesting that it was set on fire deliberately. Orange described the action as an act of "sabotage," indicating foul play.[25]

Possible reasons to use a fundamental shutdown //

→ **Plausible deniability.** An actor may want to hide the real reason for an internet shutdown.

→ **Easier to implement with local scope.** In some circumstances it might be easier to switch off a power grid for a specific local neighborhood, or power down cell towers in a targeted area, than it would be to implement a more sophisticated localized communications shutdown using other technical mechanisms.

→ **Shutdown reliability.** If you sever a cable, no messages will pass until that cable is repaired. Nor will a cell phone be of much use when all the cell towers in range are powered down. In a technical sense, fundamental shutdowns are effective. In addition, a state might not trust a third party to implement a shutdown, especially if

---

[23] Wired (2017). *How an Entire Nation Became Russia's Test Lab for Cyberwar*. Retrieved May 10, 2022, from https://www.wired.com/story/russian-hackers-attack-ukraine/.
[24] Quartz Africa (2019). *An internet cutoff during Malawi's vote count affected its electoral commission's backup network*. Retrieved May 10, 2022, from https://qz.com/africa/1625291/malawi-internet-cut-off-after-polls-close-on-election-day/.
[25] Reuters (2018). *Orange official calls Ivory Coast telecoms fire act of 'sabotage.'* Retrieved May 10, 2022, from https://www.reuters.com/article/ivorycoast-orange/update-2-orange-official-calls-ivory-coast-telecoms-fire-act-of-sabotage-idUSL5N1SM58P/.

that party is a multinational telecommunications firm headquartered in a foreign country. Authorities might instead prefer to leverage local entities, such as a power utility company, that is locally owned, or even directly under government control.

- **Fewer legislative or procedural hurdles.** It might tempt authorities struggling to assert or maintain control to shut down the internet illegally. For instance, they may instruct people loyal to a regime to sabotage a country's own communications infrastructure.

- **Immediate effect.** An authority might want a shutdown to take effect immediately, as opposed to, for example, waiting for a routing change to propagate.

- **Rogue or rebel entities.** If an actor is not authorized to order a shutdown, sabotage of communications infrastructure is the only route.

2. Routing ///

One of the earliest ways to implement a shutdown was by manipulation of network routing, which is now relatively common. This is distinct from a fundamental shutdown in that it does not entail the attack of physical telecommunications structure (such as a power grid), but instead involves internet or telecommunications implementation in the software.

It is relatively simple to implement and can be highly effective, particularly when the authorities desire to shut down all internet communications to and from nodes within their country and the outside world. How it works: routing information is altered at key points in the network infrastructure, such as at international gateways, to not pass on traffic to other infrastructure, thus causing the shutdown.

There are, however, some drawbacks to shutdown implementations based on routing. Routing changes usually take time to propagate through networks, so this technical implementation is rarely immediate. It will also take time for services to be restored when the routes are put back into their original configuration. Also, many routing protocols are designed to automatically route around outages or congestion on the communications network, and so in a sense are designed to be anti-shutdown. This is why routing may not be an effective mechanism, particularly on a localized section of the network, and is usually implemented in BGP (Border Gateway Protocol) routes for a whole nation, or very large geographic area.

Another complication is that the use of routing can lead to unintended consequences external to the jurisdiction of those implementing the shutdown. Routing routes traffic internationally, and this fact makes it difficult to implement disruptive routes without making an impact in other places.

The way shutdowns are implemented through routing is to instruct key routers to null route (also sometimes called a blackhole route, or a blackhole filter) to and from a list of ASNs (Autonomous System Numbers), the unique global identifiers for network IP (Internet Protocol) ranges within their country. Null routing means that all traffic to or from that list of ASNs will be dropped instead of being forwarded on to the next hop in the journey from the source of the communication to the destination, effectively stopping all traffic for those ASNs.

Note also that a perpetrator can use BGP routing to disrupt someone else's traffic (traffic on networks not under an authority's jurisdiction). This is known as BGP hijacking, and while sometimes malicious, it can also be accidental.[26]

Routing may have been the mechanism behind some telephony network shutdowns, but not enough information is known about those shutdowns to positively identify routing manipulation as the key mechanism. There are some challenges against routing being used for telephony shutdowns. For example, due to the evolution of telecommunications over time, from the telegraph, to analog telephony, digital trunking, VoIP, etc., telephony systems tend to utilize a more complex mix of routing mechanisms and protocols. These protocols include, but by no means are limited to: SS7, MTP, ISUP, TUP, SCCP, TCAP, TRIP, H.323, H.248, Megaco, MGCP, SGCP, SCTP, MTP1, MTP2, MTP3, M2PA, H.GCP, RTP, RTCP, SIP, Q.931, BICC, and many others.

There are many variables that contribute to determining what protocols are used, such as the carrier, carrier network architecture, the subscriber's equipment, and geographic location. Some portions of the communications path may be circuit-routed, rather than packet-routed. Multiple networks may be used for a single communication, such as an out-of-band signaling network and a voice network. Some hops of the route close to the subscriber (last mile) may be analog, while the rest of the system is digital, and so on.

This complexity in the mix of routing may be one reason why the PSTN may sometimes be left operational, while other services are shut down (although there are other reasons also, such as the continued reliance on landlines for emergency communications, and the fact that landline penetration in populations is usually small, and shrinking, in comparison to mobile phone penetration).

How to detect	Routing manipulations for the purpose of enacting a shutdown are detectable within the network.
Who can detect them	Primarily companies that track routing changes, but they are also detected by individuals running tests, whether those individuals

[26] See https://en.wikipedia.org/wiki/BGP_hijacking/ for a deeper explanation.

	are within the affected population, or external to the affected population.
Detection difficulty	**Medium.**
Possible mitigation	Unfortunately, there are few means of circumventing null routing that will prove effective. At times in the past, in circumstances where only data traffic was null routed, but voice was available, it may have been possible to utilize DoV (Data over Voice) services to circumvent. As of 2022, no such experimental services seem to remain. Note that DoV should not be confused with DoS (Data over Sound), which has no practical application for mitigation of these shutdowns. That leaves alternative infrastructure as the only viable option (see the mitigation strategies for fundamental shutdowns, above), and it should be in place before the shutdown occurs.
Cost of mitigation	**High.** This usually requires significant planning and investment of resources prior to the shutdown.
How the Helpline can assist	The Helpline cannot effectively assist in these circumstances.

Examples of routing //

➔ BGP routes

Example: On the eve of its 2016 presidential election, The Gambia experienced an internet shutdown. BGP announcement data aggregated by RIPE shows[27] the withdrawal of prefixes.

Example: Amid a coup attempt in January 2019, Gabon experienced an internet shutdown[28] for 28 hours. IODA data[29] show that around 75% of Gabon's address space was withdrawn.

[27] OONI (2016). *The Gambia: Internet Shutdown during 2016 Presidential Election*. Retrieved May 11, 2022, from https://ooni.org/post/gambia-internet-shutdown/.
[28] OONI (2019). *Internet disruption in Gabon amid coup attempt*. Retrieved May 11, 2022, from https://ooni.org/post/gabon-internet-disruption/.
[29] IODA (2019). *IODA Signals for Gabon*. Retrieved May 11, 2022, from https://ioda.caida.org/ioda/dashboard#view=inspect&entity=country/GA&lastView=overview&from=1546814820&until=1546977600/.

Example: Benin experienced an internet blackout[30] during its 2019 parliamentary elections. IODA data indicate the occurrence of a significant internet outage that began at around 10 am UTC on 28th April 2019 (the day of the election) and ended by around 6 am UTC on the next day. IODA data show that the internet blackout affected four large ASes (Authoritative Sources) in Benin.

→ **Telephony routing**

Example: We are aware of a number of shutdowns that have been implemented with telephony routing, but cannot provide a documented example, as our sources at telecommunications providers wish to remain private.

Possible reasons to use routing //

→ **Relatively easy.** This is a relatively simple way of shutting off international internet connectivity for a whole country, or for a geographic region represented by a set of ASNs.

→ **Reliable for data shutdown.** The relative simplicity of BGP and other packet-routing protocols make routing an effective way to prevent any traffic from reaching its destination given a set of ASNs or similar network range identifiers.

3. Domain Name System (DNS) manipulation ///

DNS manipulation is related to routing, but focuses on the addressing of resources in IP (Internet Protocol) communications. Perpetrators can use in-country manipulation of domain name servers, or the spoofing of DNS traffic, to direct traffic intended for specific domains, such as communications platforms like WhatsApp, away from the company's servers and instead to servers they control, or to servers that don't exist, thus causing a shutdown of the targeted services.

Given that the primary DNS servers utilized by end users are usually specified, and hosted by the users' ISP, this shutdown mechanism requires collaboration between the perpetrators (typically a government) and all the telecommunication service providers within the targeted area for the shutdown. If most of the telecommunications infrastructure is not in direct control of the government, then the shutdowns implemented with DNS manipulation are likely to be more inconsistent. Additionally, some mechanisms utilized to implement shutdowns via DNS manipulation are relatively easy for users to circumvent.

---

[30] OONI (2019). *Benin: Social media blocking and Internet blackout amid 2019 elections*. Retrieved May 11, 2022, from https://ooni.org/post/2019-benin-social-media-blocking/#internet-blackout/.

Note that there is a great deal of confusion in the naming of DNS manipulation attacks, with the same terms being used for a variety of attacks, and attacks being referred to by more than one name. Many descriptions, even from usually reliable and peer-reviewed sources such as Wikipedia, conflate different attacks on DNS into a single or paired nomenclature. For the purposes of this document, given that the primary audience are technologists working with civil society on solving issues of communications shutdown, we will adopt the Open Observatory of Network Interference (OONI) definitions as listed in their glossary.[31]

Where the state maintains its own mandated DNS servers that return false mappings of domains to IP addresses (possibly combined with blocking well known international DNS servers, such as Google's 8.8.8.8 servers, at the nation's international gateways), we will call this *"mandated local DNS hijacking."*

Where the state forces ISPs to configure their DNS servers (the default DNS servers used by all the subscribers to the ISP) to falsely respond to queries to return false mappings of domains to IP addresses, we will call these instances of *"compelled local DNS hijacking."* This is essentially the same as the previous scenario, except the ISPs own and manage the rogue DNS servers, rather than the government itself. Given the greater diversity of ISPs, this tends to lead to inconsistency of implementation.

Where DNS queries are dynamically detected on the nation's network, and rogue devices race to respond with fake responses spoofed as the intended destination DNS server, before that (authoritative) DNS server, we will call these instances of *"DNS spoofing."* Note that this type of DNS manipulation, as currently seen in China, causes collateral damage beyond China's own networks. The reason for this is it does not differentiate between DNS traffic that originates within its borders and DNS traffic that, for whatever reason, is routed via Chinese networks but originates beyond China's borders. When DNS traffic is routed through China's networks, it gets attacked, and the response is spoofed, as if the DNS request was from a local citizen. In this way, China's DNS manipulation bleeds beyond its jurisdiction.[32]

Where all DNS traffic is prevented from traversing a nation's international gateways, as is frequently done in China, we will call this *"DNS server blocking."*

Where a bad actor (not necessarily a state actor) uses some other mechanism, such as exploiting a software vulnerability, or using malware, to "poison" a resolver's cache — we will also call these instances of *"DNS hijacking,"* since the resultant effect is the same. As this attack uses exploits, and the vulnerabilities being exploited are usually patched quickly, this is not an attack a nation is going to employ as a standard procedure. If it were used by a

---

[31] OONI (2022). *OONI Glossary*. Retrieved May 11, 2022, from https://ooni.org/support/glossary/.
[32] USENIX FOCI (2014). *Towards a Comprehensive Picture of the Great Firewall's DNS Censorship*. Retrieved May 11, 2022, from https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf/.

state actor, it would likely be at a time-sensitive moment, since a hoarded zero-day exploit is going to be expended to conduct this attack.

How to detect	DNS manipulation is detectable in the network.
Who can detect them	Individuals or systems external to the affected population that have the ability to proxy DNS requests from inside the affected network and compare those results to results from outside the affected network.
Detection difficulty	**Medium.** The difficulty to detect and attribute a DNS manipulation varies depending on how it is implemented.[33]
Possible mitigation	In the case of mandated, or compelled local DNS hijacking, use trusted DNS servers beyond the control of the authorities. In the case of DNS spoofing, use a VPN and trusted DNS servers beyond the jurisdiction of the authorities (connect to the VPN servers using IP addresses, not domain names). To further protect against DNS manipulation attacks, it may help to use DNSSEC (DNS security extensions), DoT (DNS over TLS), or DoH (DNS over HTTPS). DoT and DoH encrypt the DNS traffic, and therefore may also mitigate other security issues relevant to civil society actors, such as defeating surveillance of DNS queries.
Cost of mitigation	**Low to medium.** Depending on the technique being used. A simple DNS hijacking can be circumvented by changing the resolver; meanwhile, circumventing DNS spoofing can be more difficult.
How the Helpline can assist	The Helpline can deploy mitigation strategies in these instances.

[33] For a deeper analysis of this issue, see https://ooni.org/post/not-quite-network-censorship/.

Examples of DNS manipulation //

- **Example**: OONI data have confirmed the blocking of hundreds of websites and platforms in Iran,[34] many of which are blocked by means of DNS injection.[35] OONI data also show[36] that Facebook Messenger has been blocked in Iran by means of DNS in recent years.[37]

- **Example**: At least 25 websites related to the Catalan referendum were blocked by means of DNS tampering. OONI data show[38] that these sites were blocked by means of DNS manipulation on at least two local ASes leading up to, during, and following Catalonia's 2017 independence referendum.

- **Example**: Amid protests in 2017, Pakistan blocked access to social media platforms and instant messaging apps. OONI data show[39] that they were all blocked by means of DNS tampering.

Possible reasons to use DNS manipulation //

- **Easy targeting of domain-based services.** This approach makes it particularly easy to target social media, VoIP, and messaging platforms where the authentication, call connection, or content delivery platforms are hosted on a small set of DNS domains.

4. Filtering ///

Perpetrators of internet shutdowns can use commercial filtering appliances, such as those provided by BlueCoat, Cisco, and others,[40] and transparent proxy devices, to block access to specific communications platforms, such as Facebook, Twitter, or WhatsApp. Many

---

[34] OONI (2017). *Internet Censorship in Iran: Network Measurement Findings from 2014-2017*. Retrieved May 11, 2022, from https://ooni.org/post/iran-internet-censorship/.
[35] OONI Glossary (2022). *DNS spoofing*. Retrieved May 11, 2022, from https://ooni.org/support/glossary/#dns-spoofing/.
[36] OONI Explorer (2020). *Facebook Messenger was NOT reachable in Iran*. Retrieved May 11, 2022, from https://explorer.ooni.org/measurement/20200504T201233Z_AS50810_ftkZkpp5TvmA6Kg7GN4MlJmXqdtuG3oIWWX13kFH0GUMxfKuCj/.
[37] OONI Explorer (2020). *Iran search results*. Retrieved May 11, 2022, from https://explorer.ooni.org/search?until=2020-05-05&probe_cc=IR&test_name=facebook_messenger/.
[38] OONI (2017). *Evidence of Internet Censorship during Catalonia's Independence Referendum*. Retrieved May 11, 2022, from https://ooni.org/post/internet-censorship-catalonia-independence-referendum/.
[39] OONI (2017). *How Pakistan blocked news outlets, social media sites, and IM apps amidst protests*. Retrieved May 11, 2022, from https://ooni.org/post/how-pakistan-blocked-social-media/.
[40] See https://umbrella.cisco.com/solutions/web-content-filtering/ for an example of a filter application on the market.

countries have this capability, and authorities use this mechanism frequently to implement shutdowns in China, Iran, Saudi Arabia, and elsewhere.

One "advantage" of using filtering devices is that they can be used both for censorship (of media websites, etc.) and shutdowns (of social media, VoIP, and messaging service platforms). Some governments may choose filtering devices over other shutdown mechanisms because they may see less opposition from their citizens regarding deployment of these devices. Frequently, governments cite blocking websites hosting CSAM (Child Sexual Abuse Material), and criminal websites, as the rationale for deploying filtering. This gets the equipment in place, opening the door to censoring or shutting down communications on a far greater scope than originally claimed.[41]

Filtering devices work by examining the metadata associated with communications traffic, and taking action based on that metadata. The metadata attributes commonly used for this form of censorship and shutdown include, but are not limited to: source and destination IP address, destination domain name, source and destination port, full resource path, resource file extension, etc.

Filtering devices are usually either implemented on the backbone (typically in circumstances where the government controls all the telecommunications infrastructure within a country), or mandated to be implemented by each and every carrier/ISP operating within a country. Note that if the devices are the responsibility of the ISPs, then frequently the filtering is not consistent across the whole country, since each ISP may comply with the government order in a different way, some blocking more than others (for example some may only block a sub-domain, or a full path of a service, while others block the base domain).

When a subscriber attempts to access a blocked website, the filtering devices usually return a page noting that the requested page is blocked, and citing the relevant government regulations utilized to implement the block. However, sometimes the devices are configured to redirect to an error page falsely claiming the original requested resource does not exist.

The use of filtering devices on a small scale is easy and well understood (for example, filtering devices deployed by corporations for their own networks in the workplace) and requires little maintenance. However, when implemented on a nation-wide basis, filtering devices require significant investment in the network design, deployment, and maintenance of the products. Therefore, national-scale deployments of filtering devices require knowledge, design and deployment input, and constant maintenance from the product

[41] See, e.g., American Library Association (2006). *Why Filters Won't Protect Children or Adults.* Retrieve May 12, 2022, from http://www.ala.org/advocacy/intfreedom/filtering/whyfilterswontprotect

vendor. The vendors of such products to nations cannot deny they have knowledge of the deployment, or use of their products for human rights abuse.[42] [43] [44] [45]

Filtering devices are a common choice where a product-based approach to censorship and social media or internet communications platform shutdown is desired. But such products can also be used to block everything, thus causing a complete internet shutdown.

The main weakness of filtering devices is that under normal use where a relatively small set of websites or platforms are blocked, users can easily bypass the filtering by utilizing a VPN, provided that the VPN itself is not also blocked by the filtering device.

Note also that filtering devices can be used to block MITM (Man-In-The-Middle) encrypted HTTPS traffic, but this is not common in most circumstances, since the authorities run the risk of that fact being discovered and reported, which would erode commercial and domestic trust in online banking, and other such essential services.

How to detect	Filtering devices may be detectable on the network with network fingerprinting or similar tools.
Who can detect them	Individuals within the affected population. Possibly also individuals external from the affected population, but who can proxy traffic through infrastructure within the affected network.
Detection difficulty	**Easy (if a blockpage is provided).** **Medium (when blocking is done by other means).**
Possible mitigation	In most circumstances the use of a trusted VPN will circumvent a shutdown implemented with filtering. Open HTTPS proxies located beyond the filtered network may also work.
Cost of mitigation	**Low.**

[42] The Washington Post (2013). *Report: Web monitoring devices made by U.S. firm Blue Coat detected in Iran, Sudan*. Retrieved May 11, 2022, from https://www.washingtonpost.com/world/national-security/report-web-monitoring-devices-made-by-us-firm-blue-coat-detected-in-iran-sudan/2013/07/08/09877ad6-e7cf-11e2-a301-ea5a8116d211_story.html/.
[43] CBS News (2013). *Surveillance and censorship: Inside Syria's Internet*. Retrieved May 11, 2022, from https://www.cbsnews.com/news/surveillance-and-censorship-inside-syrias-internet/.
[44] The Wall Street Journal (2011). *U.S. Products Help Block Mideast Web*. Retrieved May 11, 2022, from https://www.wsj.com/articles/SB10001424052748704438104576219190417124226/.
[45] Slashdot (2011). *Censorware Vendors Can Stop Mid-East Dealings*. Retrieved May 11, 2022, from https://yro.slashdot.org/story/11/03/29/1520247/censorware-vendors-can-stop-mid-east-dealings/.

How the Helpline can assist	The Helpline can assist with mitigation strategies in these instances.

Examples of filtering //

➔ **Application layer interference**
Commercial filtering appliances usually work with metadata at the application layer. Historically this has made them a popular choice for implementing partial shutdowns by destination address and protocol.

Example: Meta's WhatsApp platform was blocked in Brazil in December 2015, and again in May and July 2016, using application layer filtering.[46] [47]

➔ **Transparent proxying**
A transparent proxy is a server that sits between users and internet content. It is called "transparent" as it requires no configuration or knowledge from the user to utilize it, and thus for most users will be invisible to their internet experience. The transparent proxy achieves this by redirecting the users' traffic at the network layer. The proxy acts on behalf of those users, and in this way can be configured either to pass on, or block, web requests, according to its configuration. Transparent proxies were one of the first mechanisms utilized to implement censorship and shutdowns, but are no longer used in this role at national scale, as they are unable to proxy HTTPS traffic without compromising the trust relationship of the TLS cryptosystem.

Example: Saudi Arabia was known to use transparent proxying on their international gateways in the late 1990s and early 2000s.

Possible reasons to use filtering //

➔ **Easy targeting of domain-based services.** Filtering makes it relatively simple to target social media, VoIP, and messaging platforms, in particular where the authentication, call connection, or content-delivery platforms are hosted on a small set of DNS domains.

[46] TechCrunch (2016). *WhatsApp blocked in Brazil again*. Retrieved May 15, 2022, from https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/.
[47] Access Now (2022). *#KeepItOn STOP Data 2016-2021*. Retrieved May 15, 2022, from https://www.accessnow.org/keepiton-2016-2021-data/.

- **Immediate effect.** This approach is effective if the perpetrator wants the shutdown to take effect immediately, as opposed to, for example, waiting for the propagation time necessary for a shutdown implemented through routing changes to take effect.
- **Granular scope.** Filtering rules can be written to target filtering based on the locality of the subscriber. This is only limited by the granularity of geo-IP allocation mapping.
- **Ease of obtaining popular support.** Because filtering devices are multipurpose, it may be easier to get support for deployment.

5. Deep Packet Inspection (DPI) ///

Nation states typically use DPI out-of-band to carry out online surveillance, but if they use DPI inline on key network trunks or backbones, they can utilize the technology to cause shutdowns. DPI shares many of the characteristics of filtering with regard to the commercial availability of products, the need for close vendor involvement to implement and maintain the technology on a national scale, etc. DPI devices have all the capability of filtering devices, but with the added functionality of allowing rules, or heuristic approaches, based on the content of the communication, in addition to its metadata. For this reason, DPI is also able to identify when subscribers are deploying circumvention tactics such as protocol obfuscation.

Many countries have DPI infrastructure in place, often deployed ostensibly to conduct surveillance to protect national security or fight organized crime. Some countries, such as China, use DPI technology extensively inline to tear down connections on the networks that do not conform to allow-listed (also known as “whitelisted”) protocols.

Inline DPI is very challenging to implement on a national level because it introduces latency. Packets are pulled off the wire, then re-assembled according to the protocol of their higher-level communication, the content of the communication assessed according to the rules and heuristics in place, and then disassembled back into packets to be forwarded on, or if the content matches a rule, logged and the communication dropped.

How to detect	Inline DPI mechanisms enacting a shutdown are detectable in the network.
Who can detect them	Individuals within the affected population. Possibly also individuals external from the affected population, but who can proxy traffic through infrastructure within the affected network (depending on aspects of how the DPI mechanisms and the

	networks are configured).
Detection difficulty	**Medium.**
Possible mitigation	If the shutdown is implemented according to protocols, or is rules-based, then a VPN, or open HTTPS proxy located beyond the affected network, may circumvent the shutdown. In circumstances where the DPI device is heuristic, particularly where it tears down non-allow-listed protocol connections, it is far more difficult to mitigate. The use of an obfuscation proxy to hide communications inside an allow-listed protocol is the most likely strategy to work under these circumstances.
Cost of mitigation	**Medium.**
How the Helpline can assist	The Helpline can assist with mitigation strategies in these instances.

Examples of DPI mechanisms for shutdowns //

- **Example**: OONI data has shown[48] that Egyptian ISPs reset connections through the use of DPI technology. In 2016, OONI first found[49] that Egyptian ISPs were using DPI equipment to hijack unencrypted HTTP connections and redirect them to revenue-generating content, such as affiliate ads.
- **Example**: OONI data has shown[50] that Cuba uses DPI technology to shut down the Skype communications platform by injecting reset packets into the connections.
- **Example**: Amid a wave of protests in Iran during the first week of 2018, OONI data show[51] [52] that DPI technology was used to block access to the Instagram platform by altering TLS packet headers.

[48] OONI (2018). *The State of Internet Censorship in Egypt*. Retrieved May 11, 2022, from https://ooni.org/documents/Egypt-Internet-Censorship-AFTE-OONI-2018-07.pdf/.
[49] OONI (2016). *Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections?* Retrieved May 11, 2022, from https://ooni.org/post/egypt-network-interference/.
[50] OONI (2017). *Measuring Internet Censorship in Cuba's ParkNets*. Retrieved May 11, 2022, from https://ooni.org/post/cuba-internet-censorship-2017/.
[51] OONI (2018). *Iran Protests: OONI data confirms censorship events (Part 1)*. Retrieved May 11, 2022, from https://ooni.org/post/2018-iran-protests/.
[52] OONI (2018). *Iran Protests: DPI blocking of Instagram (Part 2)*. Retrieved May 11, 2022, from https://ooni.org/post/2018-iran-protests/.

Possible reasons to use DPI //

- **Targeting of services based on packet content.** Perpetrators often choose DPI because it can more thoroughly thwart common circumvention techniques. DPI can discover protocols encapsulated or hidden within other protocols, and can unpack encoded (but not encrypted) content. It can be used to interfere with, but not necessarily decrypt, encrypted protocols or content.
- **Immediate effect.** This approach is effective if the perpetrator wants the shutdown to take effect immediately, as opposed to, for example, waiting for the propagation time necessary for a shutdown implemented through routing changes to take effect.
- **Granular scope.** DPI rules can be written in a way that the device affects traffic based on the locality of the user. This is only limited by the granularity of geo-IP allocation mapping.
- **Application for secondary functions.** DPI is a powerful technology with many uses, including but not limited to: network diagnostics, network performance tuning, censorship, and surveillance. This makes DPI a primary choice as a singular solution for multi-function network monitoring and interference.

6. Rogue infrastructure attack ///

A rogue infrastructure attack is when a perpetrator introduces a mechanism (usually temporary) in the infrastructure in a locality or network segment, such that it clones the legitimate infrastructure the user would typically connect to, at least as it appears to the end users' devices. Users transparently connect their devices to the rogue infrastructure instead of the legitimate one, putting their communications in the hands of the operator of the rogue node. While this type of shutdown is not exclusively restricted to wireless forms of communication, it is most frequently implemented on radio frequency-based networks, such as mobile cellular telecommunications, and WiFi.

Note that when utilizing WiFi, bluetooth, or other ad hoc mesh technology to mitigate a shutdown, it is not feasible to prevent rogue nodes from joining your mesh networks. This is an important consideration for assessing risk when using mesh technologies in a particular context.

How to detect	Rogue infrastructure is detectable with the right applications.
Who can detect	Individuals at the location where the rogue infrastructure is

them	present.
Detection difficulty	**Hard.**
Possible mitigation	Usually the only viable mitigation in circumstances where rogue nodes are present is to stop using the communications system those rogue nodes are intercepting. Since moving to another communications platform may be inconvenient at best, and entirely impossible under other circumstances, this can be difficult to circumvent. It can work in circumstances where WiFi is being intercepted, and wired (ethernet) connectivity is available to replace the WiFi. In circumstances where the cellular network is compromised with rogue nodes, all alternative options for mobile devices are likely to be vulnerable as well. It may be possible to utilize a mesh technology, such as external mesh antennas like goTenna devices,[53] but if they are safe, it is only because the authorities have not yet deployed equipment to compromise such systems, rather than those systems being resilient to rogue infrastructure.
Cost of mitigation	**High.** This usually requires significant investment of resources to provide the diagnosis and deploy alternative infrastructure.
How the Helpline can assist	The Helpline cannot effectively assist in most of these circumstances.

Examples of rogue infrastructure attacks //

→ IMSI catcher / Rogue cell tower

Example: During the 2016 Standing Rock #NoDAPL protests in North Dakota, U.S., clients of the Helpline and other participants reported suddenly unreliable wireless signals and disconnected calls in what appeared to be a highly localized mobile shutdown.[54] [55]

[53] See https://gotenna.com/ for more information.
[54] Wetmachine (2016). *Are Police Jamming Cell Phones At Standing Rock Protest? The FCC Should Investigate*. Retrieved May 15, 2022, from https://wetmachine.com/tales-of-the-sausage-factory/are-police-jamming-cell-phones-at-standing-rock-protest-the-fcc-should-investigate/.
[55] Wired (2016). *As Standing Rock Protesters Face Down Armored Trucks, the World Watches on Facebook*. Retrieved May 15, 2022, from https://www.wired.com/2016/10/standing-rock-protesters-face-police-world-watches-facebook/.

- **Rogue WiFi access point**

  Example: We do not have proven examples of this on record.

- **Rogue router (wired environments)**

  Example: We do not have proven examples of this on record.

Possible reasons to use rogue infrastructure attacks //

- **Highly localized.** Rogue infrastructure will often have similar capability and reach as the infrastructure it is mimicking, and therefore if it is mimicking a mobile cell tower, its shutdown effect will cover a similarly localized area (usually a maximum of 5 km radius from the tower). If the rogue infrastructure was a WiFi access point, then it could be even more localized to a single building, or series of rooms.

- **Enables surveillance.** Identification of individuals at a location, such as a protest, is usually the primary motivation to utilize rogue infrastructure.

- **Hard to detect.** Rogue infrastructure mimics existing infrastructure, and from the subscribers' device point of view, and is therefore largely indistinguishable from the normal infrastructure. Very small differences need to be detected to discover that a particular piece of infrastructure is in fact rogue.

- **Rogue or rebel entities can use this approach.** Any entity not authorized to request a shutdown, may implement one through the deployment of rogue communications infrastructure.

7. Denial of Service (DoS) attack ///

Perpetrators use DDoS (Distributed Denial of Service) and other DoS (Denial of Service) attacks to target the communications of specific platforms, or even the internet communications of an entire country, as was the case in November 2016 when those behind the Mirai botnet tried unsuccessfully to shut down the submarine cable that connects the country of Liberia to the internet.[56] The offering of DDoS as a criminal service is highly organized and cheap, so if governments or other actors want to shut down a platform or network, they may utilize those third parties to conduct the attack.

[56] BBC News (2016). *Hack attacks cut internet access in Liberia*. Retrieved May 11, 2022, from https://www.bbc.com/news/technology-37859678/.

Any wireless communications technology can be disrupted with the appropriate radio frequency-jamming equipment. Perpetrators can shut down WiFi, wireless broadband, cellular telephone systems, broadcast radio, two-way radio, and satellite services in this manner. This method for shutdowns has been used in Iran, particularly to suppress satellite signals.[57] There are many techniques used in radio jamming, but it can be as simple as the powerful radio broadcasting of noise in the target frequency bands. The scale of the jamming shutdown can be controlled by the output power of the jamming transmitter.

How to detect	DDoS attacks are detectable on the network.
Who can detect them	The owner / maintainer of the service being DDoSed, the provider hosting the service, DoSP (Denial of Service Protection) providers, and telcos and companies with visibility into significant routes on the internet.
Detection difficulty	**Easy.**
Possible mitigation	The use of a DoSP (Denial of Service Protection) provider is the best strategy to mitigate a DDoS attack, but such services are much easier to set up prior to an attack than during an attack. Good free providers for DoSP for civil society organizations are available, such as Cloudflare's Project Galileo,[58] and eQualit.ie's Deflect.[59] Radio jamming, however, is essentially impossible to mitigate from a technical perspective, and would have to be dealt with through national and international regulatory bodies ensuring compliance with international agreements on radio frequency usage.
Cost of mitigation	**Low to high.** Depending on the circumstances of each case.
How the Helpline can assist	The Helpline can help with instances of DDoS, but cannot effectively assist for instances of radio frequency jamming.

[57] Small Media (2012). *Satellite Jamming in Iran: A War Over Airwaves*. Retrieved May 11, 2022, from https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf/.
[58] *See* https://www.cloudflare.com/galileo/.
[59] *See* https://equalit.ie/portfolio/deflect/.

Examples of DoS shutdowns //

➔ **DoS, DDoS**

Example: DDoS attacks took down network segments in Georgia in 2008,[60] and in Ukraine in 2014.[61] While both of these attacks were conducted at times of Russian military activity in those two countries, attribution to Russia was not conclusive.

➔ **Radio Frequency Jamming**

Example: The jamming of satellite communications networks in Iran occurred sporadically since May 2009,[62] and continuously since February 2011.[63] This jamming affects broadcast media, person-to-person communications networks, and other satellite -based systems, as was noted in July 2014 by the Iranian Meteorological Organization, with tragic consequences.[64]

Possible reasons to use DoS attacks //

➔ **Plausible deniability.** An actor may be trying to hide the intention behind a shutdown.

➔ **Avoids legislative or procedural hurdles.** An actor that does not want to meet legal or other requirements may hire criminals to cause a shutdown through DDoS attacks against communications platforms.

➔ **Tool for rogue or rebel entities.** This method gives criminals or rogue actors that do not have authority to order a shutdown a means to implement one.

➔ **Users cannot circumvent the shutdown.** Mitigation has to be effected by the service provider.

➔ **Local scope (radio frequency jamming).** Jamming of WiFi in particular can target a specific local area.

---

[60] BBC News (2014). *Russia and Ukraine in cyber 'stand-off'*. Retrieved May 15, 2022, from https://www.bbc.com/news/technology-26447200/.
[61] Mother Jones (2014). *Are Russia and Ukraine on the Verge of an All-Out Cyberwar?* Retrieved May 15, 2022, from https://www.motherjones.com/politics/2014/03/cyber-war-ukraine-russia/.
[62] Al-Monitor (2015). *Will Rouhani end jamming of satellite TV signals?* Retrieved May 15, 2022, from https://www.al-monitor.com/originals/2015/09/iran-satellite-jamming.html/.
[63] Human Rights Watch (2011). *Iran: Stop Attacks on Peaceful Demonstrators*. Retrieved May 15, 2022, from https://www.hrw.org/news/2011/02/14/iran-stop-attacks-peaceful-demonstrators/.
[64] RadioFreeEurope/Radio Liberty (2014). *Iranian Satellite Jamming Causes Storm Of Controversy*. Retrieved May 15, 2022, from https://www.rferl.org/a/iran-jamming-controversy-storm/25467735.html/.

- → **Global scope (radio frequency jamming).** If the communications being jammed operate on the lower frequency bands, then jamming can potentially affect the target frequency over very large distances, including globally.
- → **Hard to mitigate (radio frequency jamming).** The only avenue to remedy radio jamming is via national and international action.

8. Throttling ///

Throttling is the act of artificially restricting, but not stopping, the flow of data through a communications network. Throttling makes it appear as though internet access or a platform or service is available, but the level of interference is enough to make the service or resource effectively useless.

There are many technical mechanisms to throttle, or slow down, access to the internet or particular services, several of which are explored in more detail above. These include QoS (Quality of Service) throttling by protocol; managing bandwidth by source or destination IP (Internet Protocol) addresses, IP subnets, VLANs (Virtual Local Area Networks), or MAC (Media Access Control) addresses; traffic shaping and policing; inline DPI (Deep Packet Inspection) at layer 5 and above in the OSI (Open Systems Interconnection) networking model; or NIC (Network Interface Controller) / Port partitioning at layer 2 in the OSI, which affects all traffic.

An actor can apply throttling to restrict all communications on a networking path, or to restrict particular communications based on protocol, source, destination, and more.

In many parts of the world, it is difficult to distinguish between deliberate throttling and slow internet connections caused by poor network infrastructure, so throttling can be a way to "hide" an internet shutdown in plain sight.[65]

How to detect	It can be difficult to differentiate deliberate network throttling from incidental network congestion, but in some cases, those with adequate data can make an educated distinction.
Who can detect them	Companies that track internet traffic flows. Individuals who are affected by the throttling. Potentially individuals who are outside the throttled network (depending on how the throttling is

[65] Mozilla Internet Health Report (2019). *Internet slowdowns are the new shutdowns*. Retrieved from May 11, 2022, from https://internethealthreport.org/2019/internet-slowdowns-are-the-new-shutdowns/.

	implemented).
Detection difficulty	**Hard.**
Possible mitigation	When the throttling is protocol-based — that is, when an actor slows access to sites or services based on an internet protocol, such as those used for online browsing or voice calls — those impacted by the throttling may be able to regain access by using VPNs, store-and-forward communications platforms, or obfuscation proxies, or by wrapping their traffic inside another protocol not affected by the throttling. In cases where traffic is throttled by source IP address, those impacted can use a proxy with a source address that is not affected. In instances where an actor is throttling literally all internet traffic (instead of using a filter such as source or destination IP address, the protocol, etc.), circumvention is difficult, because those impacted would need to get unrestricted connectivity through an alternative infrastructure, such as by using a satellite uplink or other long-distance wireless technologies. Unfortunately, these options typically offer restricted bandwidth with high latency regardless, so such circumvention may not yield much of a gain over the throttled speed.
Cost of mitigation	**Low to high.** Depends on how the throttling is implemented.
How the Helpline can assist	In instances such as protocol-based throttling, the Helpline can help, but when all traffic is throttled, the Helpline cannot effectively assist.

Examples of throttling //

➔ **Bandwidth management / Traffic shaping and policing**
Bandwidth management, which can be done by source or destination IP addresses, IP subnets, VLANs, or MAC addresses.

Example: We have no proven examples of this on record.

➔ **Quality of Service (QoS)**
Networking technologies such as QoS are sometimes used to prioritize particular types of communication (protocols) over others, which can have the throttling effect on the deprioritized communication protocols traffic.

Example: We have no proven examples of this on record.

➔ **Inline DPI**
Inline DPI (Deep Packet Inspection) devices at layer 5 and above can be used to introduce latency.

Example: Iran has historically throttled HTTPS traffic, particularly in the lead-up to elections in the country, with reports dating back as early as the 2009 presidential election, when the Iranian government was rumored to have slowed down connection speeds, rendering the internet nearly unusable.[66]

➔ **NIC / Port partitioning**
A NIC (Network Interface Card), or / port partitioning, at layer 2, which will affect all traffic.

Example: We have no proven examples of this on record.

➔ **Routing path**
The routing path can be altered to be longer, or go through lower-capacity chokepoints in the network to create a throttling effect. Altering the routing path may also be implemented for surveillance purposes, by re-routing traffic through surveillance capability not on the natural routing paths for some traffic, which may have a throttling side effect on that traffic.

Example: In 2008, Pakistan Telecom (a government-owned ISP) attempted to censor YouTube in Pakistan by means of updating its BGP routes for the website. These new routes were announced to Pakistan Telecom's upstream providers, and from there broadcast to the whole internet. This caused all web requests for YouTube to be directed to Pakistan Telecom, which caused an hours-long outage of the website worldwide.[67]

Possible reasons to use throttling //

➔ **Plausible deniability.** The authorities can claim that they did not shut off the network.

---

[66] Collin Anderson (2013). *Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran*. Retrieved May 11, 2022, from https://arxiv.org/abs/1306.4361/.
[67] CNET (2008). *How Pakistan knocked YouTube offline (and how to make sure it never happens again)*. Retrieved May 11, 2022, from https://www.cnet.com/culture/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/.

- **Official communications.** If some branches of government share the public communications systems with domestic subscribers, then the authorities may be reluctant to cut those governmental branches completely offline, and opt for throttling instead.

- **Allows essential use.** Throttling, rather than complete shutdown, may allow for essential, and / or emergency communications to get through, but not be fast enough to allow for the rapid spread of content or an idea.

- **Push users off encrypted channels.** Throttling is sometimes used to force user communications out of encryption and into the clear, so that surveillance of the users' communications is possible.

IV. Where in the network a shutdown is implemented: an attribute to assess impact, collateral damage, and technical responsibility

One of the key tasks for technologists seeking to understand, circumvent, or document an internet shutdown is determining where in the network it has been implemented. The location of a technology in a network may even suggest its purpose. For example, DPI (Deep Packet Inspection) is a technology with benevolent and malignant uses. The primary difference between those uses is where in the network the equipment is placed.

The most benevolent use of DPI is at the leaf nodes of the internet, that is, enterprise network, government department, and NGO gateways. DPI used as IDS/IPS (intrusion detection and prevention) in the defense of those private networks is not just beneficial, but required. It should be considered negligent if a substantial private network does not implement defensive IDS/IPS, as this form of DPI is a key safeguard against sophisticated attackers, such as APTs (Advanced Persistent Threats).

As soon as DPI is moved away from the leaf nodes, and toward the trunks, backbones, and international gateways, it ceases to have any justification as a defensive technology, and thus we can be certain it is being deployed in an offensive role for surveillance, censorship, and shutdown purposes.

Where in the network a shutdown is implemented may also be useful in helping us understand how much impact the disruption has and how much damage it can cause. It also helps trace technical responsibility back to the perpetrator.

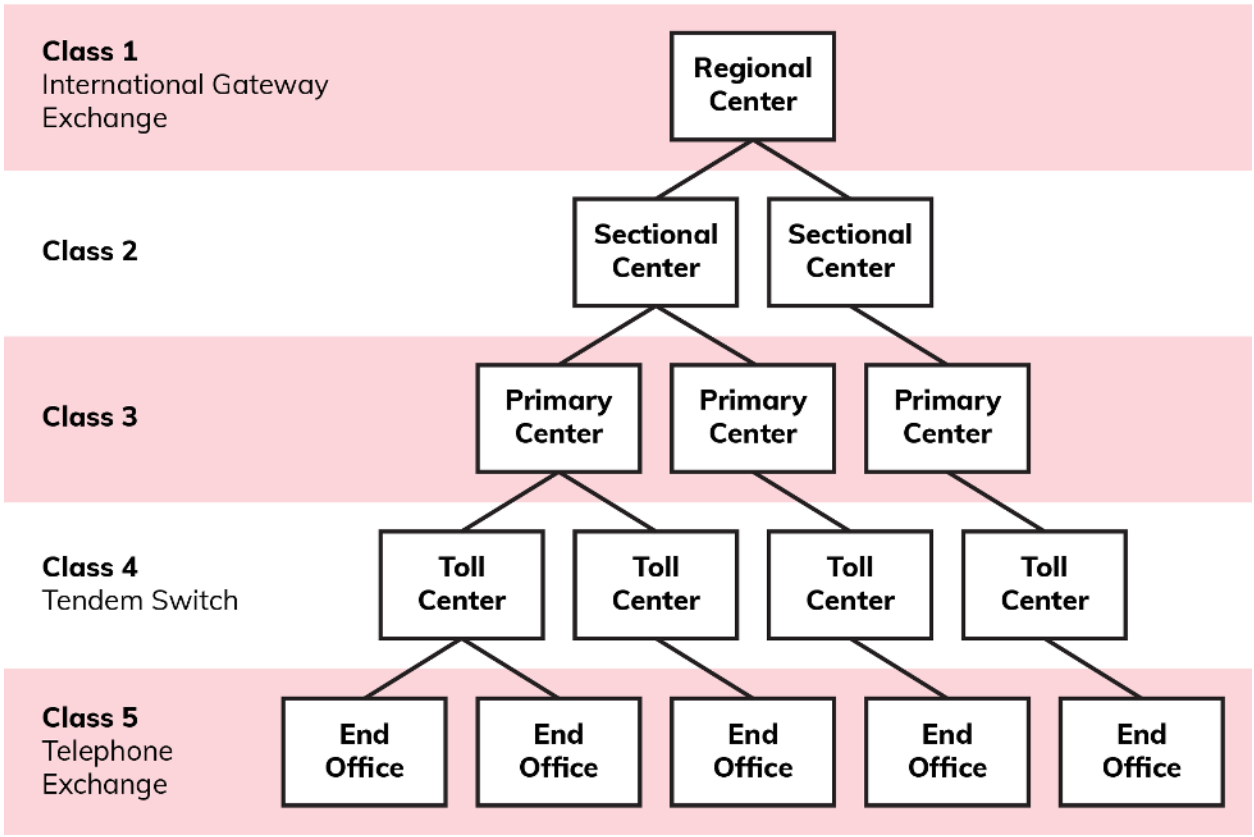
A perpetrator can implement shutdown mechanisms at the following points, among others:

- Major international backbones, or submarine cables
- International gateways
- Major national backbones
- Local ISP / Telcos
- Very localized infrastructure, e.g. a single cell tower

Following is a discussion of systems and “locations” in networked systems where perpetrators can cause disruptions.

PSTN (Public Switched Telephone Network) ///

In the PSTN, there is the Class 1-5 nomenclature of the hierarchical network topology to help characterize where in the network a shutdown has been implemented. It also helps to characterize the scale of the shutdown.



PSTN Class 1-5 nomenclature

This well-organized structure facilitates granularity of control within each telecommunications operator. A perpetrator can implement a shutdown at every scale, from the entire country down to a single mobile cell tower.

If there is any ambiguity regarding how a perpetrator has implemented the shutdown in a PSTN, it will likely be due to the different approaches one can take to technically implement a shutdown, or to the diverse interpretations a carrier might take of a shutdown order. These variations explain why subscribers to one carrier may experience more or less access during a shutdown than subscribers of another carrier.

The internet ///

Internet network topology can be difficult to characterize, given its distributed design and amorphous nature. Anyone can place devices, content, and services on it at any time. The distributed nature of the internet goes beyond physical nodes. Most aspects of the internet are also distributed in nature. That includes access to the internet, the routing of information flows, the creation and distribution of protocols and software applications, as well as logical aspects, such as control and governance.

A heuristic truth of the internet is that as traffic moves away from leaf nodes and toward more core infrastructure, that infrastructure becomes easier to define, and much less amorphous. This is true of both the physical path of data onto the "information superhighways" — such as submarine optical cables that carry data across oceans, between nations or continents — and for core services such as DNS (Domain Name System), which is a hierarchical system with a fixed number of well-known root servers at its core.

Perpetrators, typically governments, have very rarely implemented internet shutdowns on core infrastructure or services like DNS. That is likely due to the reliance of multiple nations on this vital communications infrastructure, and its cooperative management by international organizations. While there have been cases where submarine cables have been cut under suspicious circumstances and caused a significant shutdown, the governments in those situations have claimed the severing of the cables was accidental.

That is why governments are more likely to implement internet shutdowns on infrastructure within the physical geography of a nation state, or by configuring major national infrastructure to treat traffic destined for, or from, an origin outside the nation's own Top Level Domain (TLD) differently. This approach results in cutting the nation's population off from communication with international domains, which is often the goal.

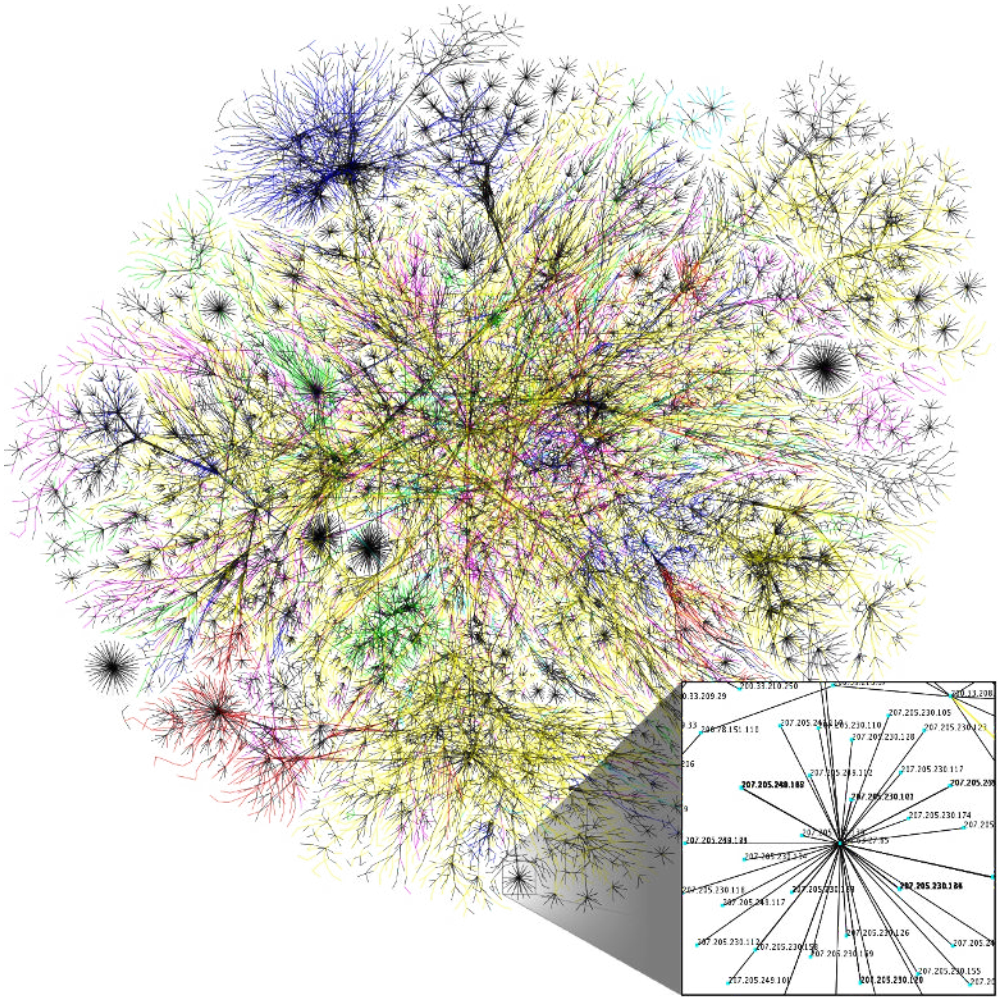
Nations that have few international internet connections are more vulnerable to shutdowns that cut them off from the international community. Tunisia, for example, has a single submarine cable that carries all the nation's internet traffic. It is therefore possible for the Tunisian government to implement a shutdown that separates its population from the rest of the world. The more international internet connections a nation has, the more work is required to implement such a complete cut-off.

Governments also use the blocking of domains and services at international gateways to force social media and communications platforms to deploy infrastructure within their geographical borders, and the legal jurisdiction of their nation. This makes it easier for the government to put these platforms within the scope of their surveillance and censorship regimes. It also allows for more granular shutdowns targeting subscribers in their country.

Most nations have major infrastructure that can be considered national backbones. Network trunks carry large amounts of the data traffic within the geographical borders of the country, either between individuals or entities inside the country, or between the subscribers to international gateways and beyond. That makes these backbones a more likely target for governments that want to disconnect the entire nation or large segments of it.

As discussed above, another way to cause shutdowns is through the deliberate or unintentional misconfiguration of BGP (Border Gateway Protocol) routes. Where in the network the perpetrator implements these misconfigurations depends on what ASNs

(Autonomous System Numbers) the configuration relates to. We have seen shutdowns where the government uses BGP routing to route traffic for one nation through another nation, most likely for the purposes of surveillance. We have also seen accidental misconfiguration, such as the misconfiguration that took Facebook offline in 2021,[68] [69] making it disappear from the internet for several hours. That was an accident that took place in the network toward a leaf node, but impacted Facebook traffic globally.



Classic style internet map[70]

Those seeking to implement more granular shutdowns will move closer to the leaf nodes of the user devices. There is often a legacy link between the delivery of PSTN infrastructure

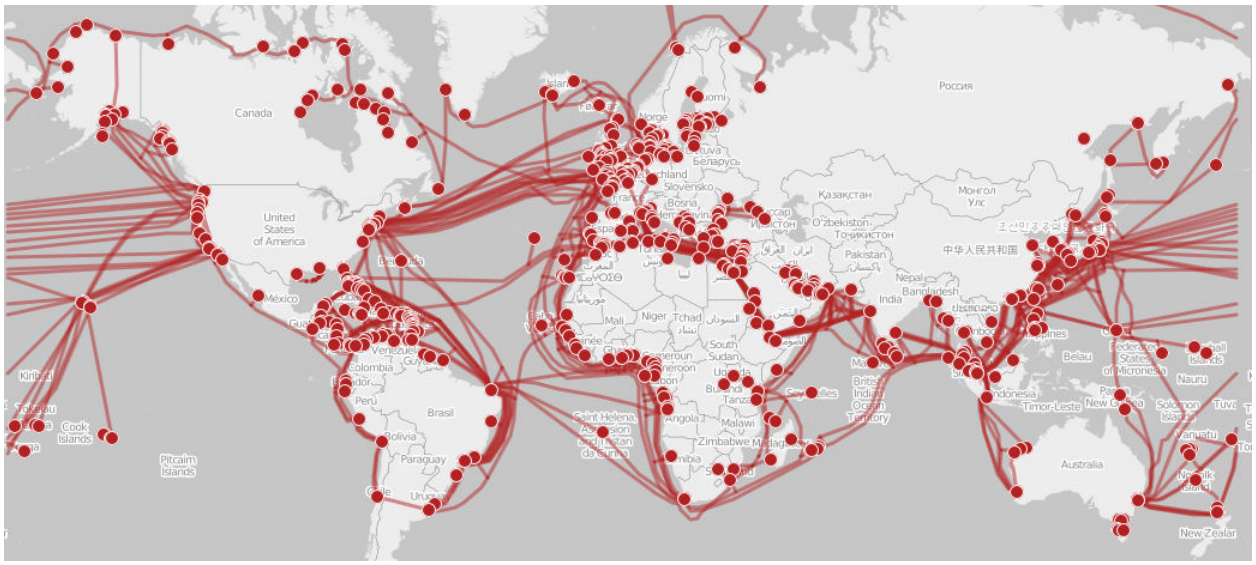
[68] Network Computing (2021). *BGP Config Change, Not Cyber Attack, Brought Down Facebook*. Retrieved May 15, 2022, from https://www.networkcomputing.com/networking/bgp-config-change-not-cyber-attack-brought-down-facebook/.

[69] The Cloudflare Blog (2021). *Understanding How Facebook Disappeared from the Internet*. Retrieved May 15, 2022, from https://blog.cloudflare.com/october-2021-facebook-outage/.

[70] By The Opte Project (2005). CC BY 2.5, Retrieved May 31, 2022, from https://commons.wikimedia.org/w/index.php?curid=25698718

and internet connectivity (via land lines, cable modems, etc., or via the cellular mobile phone network), so it is there, in the delivery of that "last mile" connectivity by telecommunications carriers, that authorities will order a shutdown implemented. It is therefore, once again, telecommunications carriers that must perform the technical implementation of shutdowns at the behest of governments. This enables authorities to plunge specific groups of internet subscribers into the dark.

There is, however, a new trend toward more amorphous delivery of "last mile" connectivity. Emerging technologies that can cross borders, such as Starlink,[71] challenge the status quo. The same is true of systems to enable subscribers to share connectivity, such as we see now with Amazon's Sidewalk protocol,[72] the Helium Network[73] with its cryptocurrency-backed network sharing system, and the proliferation of dVPNs (Distributed Virtual Private Networks),[74] where the VPN is delivered through all the subscribers utilizing the product. This type of connection sharing is likely set to explode with the deployment of 5G technology, since the technical limitations for 5G relate to the expense of deploying infrastructure to obtain coverage for technology with a very short wireless range. This facilitation of connection sharing is likely to reduce control and the granular accuracy of shutdown implementation.



Submarine cables connecting nations of the world[75]

[71] See https://www.starlink.com/satellites/.
[72] Electronic Frontier Foundation (2021). Understanding Amazon Sidewalk. Retrieved May 15, 2022, from https://www.eff.org/deeplinks/2021/06/understanding-amazon-sidewalk/.
[73] See https://www.helium.com/.
[74] See, e.g., https://sentinel.co/dvpn/.
[75] This map was created from OpenStreetMap project data, collected by the community. CC-BY-SA-2.0, Retrieved May 31, 2022, from https://en.wikipedia.org/wiki/File:Submarine_cable_map_umap.png

V. Scope: The intended and actual scope of a shutdown helps define its impact on affected populations

Technologists assessing the impact of shutdown will consider its scope. The scope of a shutdown is a measure of the services that are affected, as well as the context-specific impact the removal of those services has on affected populations. Many factors contribute to a shutdown's overall scope.

In some circumstances the implementation method a perpetrator uses to effect a shutdown has consequences beyond the communications system itself. For example, if authorities cut off internet access by turning off the electricity grid in an area, the impact goes well beyond the absence of the communications system. Any system that requires power will also be affected. This increases the scope of impact, and can create dangerous, even life-threatening situations. If the street lights are out, the chances of vehicular accidents increases. If homes cannot be heated and it is winter, the old and frail may die of hyperthermia, and so on.

A technologist assessing scope should ask: Does the shutdown affect a single platform, multiple platforms, or all communication platforms? If the shutdown only affects a single platform, are other similar platforms still available for the affected population to communicate? If a shutdown is targeting a communications platform, like Brazil's shutdown of WhatsApp in 2016,[76] then subscribers can sometimes migrate to another platform. In Brazil we saw huge numbers of WhatsApp subscribers move to Viber, and other similar communications platforms. To some degree this limits the scope of the impact for the population, even as the impact to the targeted platform is severe. If, however, authorities are ordering the shutdown to prevent the population from communicating, they will usually target multiple platforms, or even attempt to block them all. The scope in a multi-platform or all-platform shutdown is far greater, as communication alternatives will be few or non-existent.

Another important factor for assessing scope is the service penetration for the population targeted by the shutdown. Context can greatly change the scope of impact of a shutdown. For example, in most contexts, a perpetrator's interference with the use of VHF (Very High Frequency) and UHF (Ultra High Frequency) radios would not significantly affect the communications of most members of the population. But in certain rural communities, a shutdown like that could knock out a primary means of communication.

[76] See *supra* note 46.

In addition to looking at the penetration of a particular communications service or technology, technologists should take into consideration to what extent the system is relied upon for various purposes. We should be asking how important is the communication system to the impacted population for:

- Person-to-person communications;
- The utilization or dissemination of social and government services;
- The facilitation of commerce;
- Access to independent news; or
- Contacting emergency services.

The degree to which people are relying on the platform or platforms for these important functions matters for gauging the scope of impact for that particular population.

VI. Scale: The size of the affected population is a major factor in determining shutdown impact

When examining the scale of an internet shutdown, we should consider the size of the impact, particularly in terms of the raw number of people affected by the disruption, as well as what percentage the affected population represents of the population as a whole. While the scale of a shutdown is often related to where in the network it is implemented, and the size of the geographic area the shutdown impacts, scale is probably better characterized by examining the number of people affected, particularly when comparing that to the total population.

If a government implements a shutdown at the nation's international gateways, it would hint at a scale that would affect the entire population's communication with the global community. But this may not necessarily be the case. It is possible for a nation to implement "bandwidth management" at an international gateway, but use source and / or destination IP range filters to target only a small domestic geographical region. In this scenario, calculating the number of people affected and comparing that to the total national population will give you a more accurate indication of impact.

A shutdown can be nationwide, or impact a state or province, a city or town area, individual neighborhoods or similar-sized locations, or even single venues, as we saw with the shutdown of communications on the BART train system in San Francisco in 2011,[77] the cuts in the vicinity of polling stations in Borneo in 2013,[78] and the local shutdown during the referendum vote for independence in Catalonia in 2017.[79] It's important to be accurate about the number of people impacted:, a shutdown implemented in a localized area during a protest march is likely to affect more people than would normally be in that location.

Addendum: Organizations and tools for detecting and documenting shutdowns

As we note above, there are a number of organizations doing important work to monitor and document internet shutdowns, and often these organizations are working using open protocols and sharing their data to improve our collective understanding of network disruptions worldwide. Technologists eager to learn more can refer to the following public data sources and applications:

- ➔ Internet Outage Detection and Analysis (IODA)
- ➔ RIPE
- ➔ Oracle Internet Intelligence Map
- ➔ Google Product Traffic data (Google Transparency Reports)
- ➔ M-Lab data
- ➔ Route Views Project
- ➔ Snoopsnitch

[77] Scientific American (2011). *How Did BART Kill Cellphone Service?* Retrieved May 15, 2022, from https://www.scientificamerican.com/article/how-did-bart-kill-cellpho/.
[78] According to cases received by Access Now's Digital Security Helpline in 2013.
[79] openDemocracy (2017). *How technology powered the Catalan referendum*. Retrieved May 15, 2022, from https://www.opendemocracy.net/en/can-europe-make-it/how-technology-powered-catalan-referendum/.

You can measure the blocking of websites and apps using the following tools and datasets:

- ➔ OONI: OONI Probe and OONI data
- ➔ Censored Planet
- ➔ ICLab: Centinel

Glossary

0-day exploit: See *Zero-day exploit:*

AM: Amplitude Modulation. AM is a method of transmitting information, such as an audio signal, over radio waves. The information is transmitted by varying the signal strength of a carrier wave. AM is one of the main methods of transmitting the information of radio broadcasting stations.

APT: Advanced Persistent Threat. An APT is a stealthy cyber threat actor that often combines multiple sophisticated attack techniques over an extended period of time to achieve very specific, hard-to-achieve goals. Most APTs are nation state or sponsored pro-state actors.

BGP: Border Gateway Protocol. The Border Gateway Protocol is one of the primary ways data is routed on the internet, particularly on national backbones, and for international links.

BICC: Bearer-Independent Call Control. A networking protocol similar to ISUP, used for narrowband ISDN services. BICC is defined in ITU-T Recommendation Q.1970.[80]

CB: Citizens Band. CB are radio frequency bands allocated for low power, two-way radio use by ordinary citizens without the need for a license. The frequency bands available vary from country to country, with the most common being 27MHz. Some countries, such as Australia, also allocate a UHF band to CB.

CSAM: Child Sexual Abuse Material. Illegal sexual content made using minors.

DNS: Domain Name System. DNS is the primary mechanism that provides addressing of internet resources so that user devices can locate and interact with content on the internet.

[80] See https://www.itu.int/rec/T-REC-Q.1970-200609-I/en/.

DPI: Deep Packet Inspection. DPI is the act of observing data-packet network traffic by reassembling all the packets in each communication, then analyzing the communication in its entirety, often involving additional steps, such as, for example, extracting attachments from emails, decompressing them, and examining the file contents. DPI devices can be utilized "in-line" or "out-of-band," and is the fundamental mechanism utilized in IDS and IPS devices.

Exploit: A piece of computer code written to take advantage of a specific vulnerability in computer software or hardware.

Firewall: A firewall is a networking device that, according to a set of configured rules, prevents malicious or unwanted traffic from passing through it.

FM: Frequency Modulation. FM is a method of transmitting information, such as an audio signal, over radio waves. The information is transmitted by varying the signal frequency of a carrier wave. FM is one of the main methods of transmitting the information of radio broadcasting stations.

GHz: Gigahertz. Gigahertz is a unit of measurement of frequency with 1 GHz equalling 1 billion Hertz.

H.248: An implementation of H.GCP, the media gateway control protocol architecture, which provides a mechanism for seamless provision of telecommunication services between PSTN and packet networks. H.248 is defined in RFC2805,[81] RFC3015,[82] RFC3525,[83] and RFC5125.[84]

H.323: Protocol for the transmission of multimedia, such as video streaming, over packet networks. H.323 is an ITU recommendation.[85]

H.GCP: The media gateway control protocol architecture is a methodology for interfacing PSTN and packet networks.

HTTP: Hypertext Transfer Protocol. a foundational protocol for the World Wide Web.

HTTPS: Hypertext Transfer Protocol Secure. A communications protocol for secure communication over a computer network.

---

[81] See https://datatracker.ietf.org/doc/html/rfc2805/.
[82] See https://datatracker.ietf.org/doc/html/rfc3015/.
[83] See https://datatracker.ietf.org/doc/html/rfc3525/.
[84] See https://datatracker.ietf.org/doc/html/rfc5125/.
[85] See https://www.itu.int/rec/T-REC-H.323/.

IDS: Intrusion Detection System. An IDS is a system that utilizes DPI (Deep Packet Inspection) with a set of rules or signatures, or heuristic anomaly detection mechanisms, to detect complex and sophisticated cyber attacks.

IETF: The Internet Engineering Task Force.[86] An internet standards body operating as part of the Internet Society.[87]

IMSI: International Mobile Subscriber Identity. Transmitted to a carrier when placing a call or browsing the web.

In the wild: Usually refers to the use of an exploit to compromise computers connected to the public Internet.

IODA: Internet Outage Detection and Analysis (IODA)[88] is a system designed and run by the Center for Applied Internet Data Analysis (CAIDA). IODA gathers and analyzes data to detect and document internet outages.

IP: Internet Protocol, one of the base protocols that most internet communications utilize.

IPS: Intrusion Prevention System. Essentially this is an IDS (Intrusion Detection System) that works with a Firewall in real time to alter the firewall rules if the IDS detects an intrusion.

ISDN: Integrated Services Digital Network. ISDN is a suite of standards for transmission of voice and data over digital telecommunications networks.

ISP: Internet Service Provider. Any provider of internet connectivity directly to domestic or business users.

ISUP: Integrated Services (Digital Network) User Part is a subset of SS7, the suite of protocols used to set up and route telephone calls over the PSTN.

M2PA: MTP2-User Peer-to-Peer Adaptation protocol. Part of the SS7 protocol suite handling peer-to-peer MTP3 messaging. M2PA is defined in RFC4165.[89]

MGCP: Media Gateway Control Protocol. An early protocol for handling media across packet and PSTN networks. See *H.248*.

MHz: Megahertz. Megahertz is a unit of measurement of frequency with 1 MHz equalling 1 million Hertz.

---

[86] IETF (2022). *The Internet Engineering Task Force*. Retrieved May 11, 2022, from https://ietf.org/.
[87] Internet Society (2022). *The Internet Society*. Retrieved May 11, 2022, from https://www.internetsociety.org/.
[88] See *supra* note 14.
[89] See https://datatracker.ietf.org/doc/html/rfc4165/.

MITM: MITM, or Man-In-The-Middle, refers to an attack on a communications system where the malicious party has the ability to intercept communications between two other parties, and pass on the communications to the intended recipient, usually without that recipient knowing that the malicious party intercepted the communications. Potentially, the malicious MITM party may eavesdrop on the communications, tamper with the content of the messages, replay old messages, impersonate other parties, or drop messages.

MTP: Message Transfer Part. MTP is a protocol used for the provision of unduplicated message reliability in the SS7 protocol suite.

MTP1: Message Transfer Part Level 1. MTP1 is the portion of MTP handling the physical layer of the telephony networking stack.

MTP2: Message Transfer Part Level 2. MTP2 is the portion of MTP handling the data link layer of the telephony networking stack.

MTP3: Message Transfer Part Level 3. MTP3 is the portion of MTP handling the network layer of the telephony networking stack.

Megaco: Media Gateway Control protocol. IETF designation for H.248. See *H.248*.

NIC: Network Interface Card. Hardware, whether a separate "card," or integrated onto a device motherboard, that provides the physical connection to a communications network, such as an ethernet port, or a WiFi radio.

Null route: A null route is a route path configured to drop all traffic for a destination without passing the traffic on, and without sending any delivery error back to the sender. Null routes are sometimes also referred to as black hole routes, as they mimic cosmic black holes, silently consuming network traffic which is never seen again.

OONI: Open Observatory of Network Interference. OONI[90] is an organization that develops technology to measure censorship and shutdowns events.

POTS: Plain Old Telephone Service. See *PSTN*.

PSTN: Public Switched Telephone Network. The PSTN generally refers to the landline voice and data telecommunications network.

Q.931: The connection control signaling protocol of the ISDN protocol suite, as defined by ITU-T Recommendation Q.931.[91]

---

[90] OONI (2022). *Open Observatory of Network Interference*. Retrieved May 11, 2022, from https://ooni.org/.
[91] See https://www.itu.int/rec/T-REC-Q.931/.

QoS: See *Quality of Service*.

Quality of Service: A mechanism found in most routing, switching, or gateway equipment, that can be configured to prioritize bandwidth for some types of traffic over other types. Most often this is done based on the traffic protocols.

RIPE: Réseaux IP Européens Network Coordination Centre.[92] The regional internet registry for Europe, the Middle East, and some areas of Central Asia.

RTCP: RTP Control Protocol. RTCP is a control protocol for use with RTP sessions, and is defined by RFC3550.[93]

RTP: Real-time Transport Protocol. RTP is a protocol for the transmission of media, such as audio and video, over IP networks. RTP is defined by RFC1889[94] and RFC3550.[95]

SCCP: Skinny Client Control Protocol. SCCP is a proprietary protocol from Cisco Systems, which provides similar functionality to the open MGCP standard, but interfaces closely with Cisco's CallManager.

SCTP: Stream Control Transmission Protocol. SCTP is part of the IP suite, and provides messaging reliability features for UDP communications. SCTP was standardized by the IETF, and is defined in RFC4960.[96]

SGCP: Simple Gateway Control Protocol. SGCP forms part of the VoIP protocol suite, although it has largely been replaced by MGCP.

SIP: Session Initiation Protocol. SIP is a real-time protocol for handling voice calls, as well as media such as video, in some IP telephony systems. SIP is defined in RFC2543[97] and RFC3261.[98]

SMS: Short Message Service. SMS is a service facilitating the transmission of short text messages in telephone systems, including mobile phones, that was defined as part of the GSM standards.

SS7: Signaling System No. 7. SS7 is a suite of protocols for setting up and tearing down telephone calls in the PSTN. SS7 is defined in ITU-T Recommendation Q.700.[99]

---

[92] RIPE NCC (2022). *Réseaux IP Européens Network Coordinate Centre*. Retrieved May 11, 2022, from https://www.ripe.net/.
[93] See https://datatracker.ietf.org/doc/html/rfc3550/.
[94] See https://datatracker.ietf.org/doc/html/rfc1889/.
[95] See https://datatracker.ietf.org/doc/html/rfc3550/.
[96] See https://datatracker.ietf.org/doc/html/rfc4960/.
[97] See https://datatracker.ietf.org/doc/html/rfc2543/.
[98] See https://datatracker.ietf.org/doc/html/rfc3261/.
[99] See https://www.itu.int/rec/T-REC-Q.700/.

STOP: Shutdown Tracker Optimization Project. STOP is a database, maintained by Access Now, of information relating to communications shutdowns. Access Now has published a document outlining the methodology used by STOP.[100] The STOP data is also available in Microsoft XLSX format.[101]

TCAP: Transaction Capabilities Application Part protocol. TCAP is part of the SS7 suite of protocols. It handles concurrency between dialogs between sub-systems on telephony infrastructure. TCAP is defined in ITU-T Recommendation Q.771,[102]ITU-T Recommendation Q.772,[103] ITU-T Recommendation Q.773,[104] ITU-T Recommendation Q.774,[105] and ITU-T Recommendation Q.775.[106]

TLD: Top Level Domain. TLDs are the portion of domain names at the highest level of the DNS hierarchy. For example, com, org, net, biz, and so on.

TLS: Transport Layer Security. TLS is a cryptographic protocol that provides privacy and security of communications over IP networks. The current version of TLS is 1.3, and is defined in RFC8446.[107]

TRIP: Telephony Routing over IP. TRIP is a telephony routing protocol based on BGP, but where BGP routes internet traffic, TRIP routes telephony calls and messages. TRIP is defined in RFC3219.[108]

TUP: Telephone User Part. TUP is a protocol that provides conventional PSTN services across SS7 networks. TUP is defined in ITU-T Recommendation Q.771, ITU-T Recommendation Q.772, ITU-T Recommendation Q.773, ITU-T Recommendation Q.774, and ITU-T Recommendation Q.775.

UHF: Ultra High Frequency. UHF is the radio frequency band between 300 MHz and 3 GHz. The use of UHF varies greatly from country to country, but does include the 70cm and 23cm Amateur radio bands, 900MHz and 2.4GHz ISM bands (including WiFi), DECT cordless telephone band, and satellite services. In some countries it will also include broadcast TV services, and UHF CB (Citizens Band) radio channels.

---

[100] Access Now (2022). *Read Me: How to view the Access Now Internet Shutdown Tracker*. Retrieved May 11, 2022, from https://www.accessnow.org/keepiton-2020-data-methodology/.
[101] See *supra* note 4747.
[102] See http://www.itu.int/rec/T-REC-Q.771/.
[103] See http://www.itu.int/rec/T-REC-Q.772/.
[104] See http://www.itu.int/rec/T-REC-Q.773/.
[105] See http://www.itu.int/rec/T-REC-Q.774/.
[106] See http://www.itu.int/rec/T-REC-Q.775/.
[107] See https://datatracker.ietf.org/doc/html/rfc8446/.
[108] See https://datatracker.ietf.org/doc/html/rfc3219/.

UTC: Coordinated Universal Time. UTC is the main time standard used to regulate clocks and time around the world. Server-side computer systems frequently log timestamps into log files in UTC rather than local time, since variances in local time can confuse correlating logs from one server in one location with another in another location (e.g. for the purposes of collecting digital forensic evidence of a cyber attack, or similar).

VHF: Very High Frequency. VHF is the radio frequency band between 30 MHz and 300 MHz. The use of VHF varies greatly from country to country, but does include FM radio broadcasting, the 6 meter, 2 meter, and 1.2 meter Amateur radio bands, and often will include bands for TV services, radio controlled models, and many other services.

Virtual Private Network (VPN): A Virtual Private Network is a network we can access to connect to the Internet via an encrypted tunnel. Our ISP, or anyone sniffing on the free WiFi we are using to access the web, can only see our connection to the VPN service, while the website we are visiting will only record a connection from the VPN servers.

VLAN: Virtual Local Area Network refers to the practice of segmenting a single physical network into smaller virtual networks, usually for the purpose of applying access controls, or isolating traffic paths.

VPN: See *Virtual Private Network (VPN)*.

Zero-day exploit: An exploit for a vulnerability that is not publicly known. No patch or mitigation will be available from the developer of the vulnerable system, as they also are most likely unaware the vulnerability exists. When a zero-day exploit is used to compromise systems in the wild, there is a good chance the attack, the vulnerability, and the existence of the exploit will be discovered. At this point the exploit loses its zero-day status. See also *Exploit*.

A TAXONOMY OF INTERNET SHUTDOWNS: THE TECHNOLOGIES BEHIND NETWORK INTERFERENCE

#KeepItOn